

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

11.5.2004

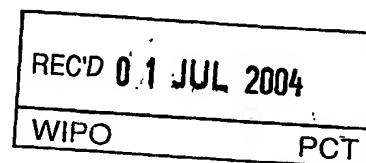
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2003年 6月 9日

出 願 番 号  
Application Number: 特願2003-163723  
[ST. 10/C]: [JP2003-163723]

出 願 人  
Applicant(s): ソニー株式会社

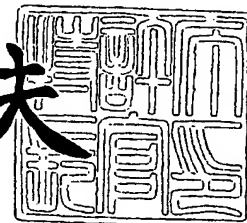


PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年 6月11日

特許庁長官  
Commissioner,  
Japan Patent Office

今井康夫



【書類名】 特許願

【整理番号】 0390433003

【提出日】 平成15年 6月 9日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/16

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 高島 芳和

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 木谷 聡

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 米満 潤

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 村松 克美

【発明者】

    【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社  
                                内

    【氏名】 浅野 智之

【特許出願人】

    【識別番号】 000002185

    【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100093241

【弁理士】

【氏名又は名称】 宮田 正昭

【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100101801

【弁理士】

【氏名又は名称】 山田 英治

【電話番号】 03-5541-7577

【選任した代理人】

【識別番号】 100086531

【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 048747

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報記録媒体、およびデータ処理方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項 1】

暗号化コンテンツを格納した情報記録媒体であり、  
コンテンツと、情報記録媒体の製造ルートのエンティティに対応して設定されたエンティティコードを格納し、一定の暗号処理単位毎に設定した暗号処理鍵生成情報としてのシードに基づいて生成する鍵によって前記暗号処理単位に含まれるデータに暗号化を施した構成を有するとともに、

前記エンティティコードを前記シードの設定領域に重複させることなく、シードに基づいて生成する鍵によって暗号化する暗号化領域に格納した構成を有することを特徴とする情報記録媒体。

【請求項 2】

前記暗号処理単位は、複数パケットの集合データ領域として設定され、

前記シードは、前記暗号処理単位の先頭パケットの先頭データから予め定められたビット数のデータを抽出したデータとして設定される構成であり、

前記エンティティコードは、パケット内のペイロードとして格納するとともに、前記シードの構成ビット領域に重複しないデータ領域に格納した構成であることを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 3】

前記エンティティコードは M P E G 規格において規定されるプログラムマップテーブル (PMT) に格納され、前記エンティティコードを前記プログラムマップテーブル (PMT) のプログラム情報領域内で、かつプログラムマップテーブル (PMT) を格納する複数の分割パケットの先頭パケットの構成データとしたことを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 4】

前記複数の分割パケットの先頭パケットは 183 バイトのペイロードを有するトランスポートストリームパケットであり、前記エンティティコードはプログラ

ムマップテーブル (PMT) のプログラム情報領域内で、かつ、プログラムマップテーブル (PMT) の先頭データから 1 8 3 バイト以内のデータとして格納した構成を有することを特徴とする請求項 3 に記載の情報記録媒体。

【請求項 5】

前記エンティティコードは M P E G 規格において規定されるプログラムマップテーブル (PMT) に格納され、

前記プログラムマップテーブル (PMT) を、複数のトランスポートストリームパケットのペイロードとして分割格納し、該トランスポートストリームパケットにさらにタイムスタンプ情報を設定したソースパケットとして情報記録媒体に分散格納した構成を有することを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 6】

前記情報記録媒体は、前記暗号化処理単位毎に設定された鍵生成情報としての第 1 シードと、

前記第 1 シードに基づいて生成される第 1 ブロックキー K b 1 に基づいて暗号化された鍵生成情報としての暗号化第 2 シードと、

前記第 2 シードに基づいて生成される第 2 ブロックキー K b 2 に基づいて暗号化された暗号化コンテンツと暗号化エンティティコードとを含む構成であることを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 7】

前記エンティティコードは、

編集スタジオコード (A S C : Authoring Studio Code) と情報記録媒体製造者コード (D M C : Disc Manufacturer Code) を含む構成であることを特徴とする請求項 1 に記載の情報記録媒体。

【請求項 8】

情報記録媒体に対する書き込みデータを生成するデータ処理方法であり、

情報記録媒体の製造ルートのエンティティに対応して設定されたエンティティコードの書き込み位置を制御して制御情報テーブル中に設定するエンティティコード設定ステップと、

前記制御情報テーブルを分割格納した複数のパケットを生成するテーブル情報

格納パケット生成ステップと、

前記テーブル情報格納パケットをコンテンツ格納パケット列に分散配置するステップと、

一定の暗号処理単位毎に設定した暗号処理鍵生成情報としてのシードに基づいて生成する鍵によって前記暗号処理単位に含まれるデータの暗号化処理を実行するステップとを有し、

前記エンティティコード設定ステップにおいては、

前記エンティティコードを前記シードの設定領域に重複させることなく、シードに基づいて生成する鍵によって暗号化される暗号化領域に含まれるように制御する処理を実行するステップを含むことを特徴とするデータ処理方法。

#### 【請求項 9】

前記暗号処理単位は、複数パケットの集合データ領域であり、前記シードは前記暗号処理単位の先頭パケットの先頭データから予め定められたビット数のデータであり、

前記エンティティコード設定ステップは、

前記エンティティコードを、前記シードの構成ビット領域に重複しないデータ領域に設定するステップを含むことを特徴とする請求項 8 に記載のデータ処理方法。

#### 【請求項 10】

前記エンティティコード設定ステップは、

MPEG 規格において規定されるプログラムマップテーブル (PMT) のプログラム情報領域内で、かつプログラムマップテーブル (PMT) を格納する複数の分割パケットの先頭パケットの構成データとなる位置に、前記エンティティコードを設定する処理を実行することを特徴とする請求項 8 に記載のデータ処理方法。

#### 【請求項 11】

前記複数の分割パケットの先頭パケットは 183 バイトのペイロードを有するトランスポートストリームパケットであり、

前記エンティティコード設定ステップは、

前記エンティティコードをプログラムマップテーブル (PMT) のプログラム情報領域内で、かつ、プログラムマップテーブル (PMT) の先頭データから 183 バイト以内のデータとして設定することを特徴とする請求項 10 に記載のデータ処理方法。

#### 【請求項 12】

情報記録媒体に対する書き込みデータを生成する処理を実行するコンピュータ・プログラムであり、

情報記録媒体の製造ルートのエンティティに対応して設定されたエンティティコードの書き込み位置を制御して制御情報テーブル中に設定するエンティティコード設定ステップと、

前記制御情報テーブルを分割格納した複数のパケットを生成するテーブル情報格納パケット生成ステップと、

前記テーブル情報格納パケットをコンテンツ格納パケット列に分散配置するステップと、

一定の暗号処理単位毎に設定した暗号処理鍵生成情報としてのシードに基づいて生成する鍵によって前記暗号処理単位に含まれるデータの暗号化処理を実行するステップとを有し、

前記エンティティコード設定ステップは、

前記エンティティコードを前記シードの設定領域に重複させることなく、シードに基づいて生成する鍵によって暗号化される暗号化領域に含まれるように制御する処理を実行するステップを含むことを特徴とするコンピュータ・プログラム。

#### 【発明の詳細な説明】

##### 【0001】

##### 【発明の属する技術分野】

本発明は、情報記録媒体、およびデータ処理方法、並びにコンピュータ・プログラムに関する。詳細には、コンテンツを記録した情報記録媒体の不正コピーに基づく不正なコンテンツ利用を防止する情報記録媒体、およびデータ処理方法、並びにコンピュータ・プログラムに関する。

## 【0002】

## 【従来の技術】

昨今、音楽等のオーディオデータ、映画等の画像データ、ゲームプログラム、各種アプリケーションプログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはCD（Compact Disc）、DVD（Digital Versatile Disc）、MD（Mini Disc）等の情報記録媒体（メディア）を介して流通している。これらの流通コンテンツは、ユーザの所有するPC（Personal Computer）、CDプレーヤ、DVDプレーヤ、MDプレーヤ等の再生装置、あるいはゲーム機器等において再生され利用される。

## 【0003】

音楽データ、画像データ等、多くのコンテンツは、一般的にその作成者あるいは販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、コンテンツの利用を許諾し、許可のない複製等が行われないようにする構成をとるのが一般的となっている。

## 【0004】

特に、近年においては、情報をデジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことが可能であり、不正コピーコンテンツのインターネットを介した配信や、コンテンツをCD-R等にコピーした、いわゆる海賊版ディスクが大量に流通しているという問題がある。

## 【0005】

近年開発されたDVD等の記録媒体では、1枚の媒体に例えば映画1本分の大量のデータをデジタル情報として記録することが可能であるが、このように映像情報等をデジタル情報として記録することが可能となると不正コピーを防止して著作権者の保護を図ることが益々重要になってくる。

## 【0006】

映画コンテンツの不正な複製行為が現実には発生しており、HD（High D

efinition) デジタル・ビデオカメラやHDデジタルビデオディスク記録の民生市場での実用化が見込まれる中で、この状況を解決せずに放置することは、著作権者の利益確保に深刻な影響を及ぼす事態を招くことは想像に難くない。

#### 【0007】

不正な複製行為の事例としては、たとえば以下に示すようなものがある。

##### <1. 映画館での撮影・盗難、コンテンツ所有者からの窃盗>

映画館で上映される新作の映画をデジタル・ビデオカメラで撮影し、これをソースとしてROM化されたDVD-Videoを製造することが行われている。また、映画館で上映するフィルムをその価値に見合う対価を支払うことなく、かつ権利保有の許諾を得ることなくテレシネ作業によりベースバンド・ビデオ信号へ変換し、これをソースとしてROM化された海賊版DVD-Videoを製造することが可能である。

#### 【0008】

さらには、コンテンツ所有者からフィルムをテレシネ変換しHDDへ記録するなどされてコンテンツが盗難に会う場合もある。このコンテンツをDVD製造工場へ持ち込むことでROM化されたDVD-Videoを製造することも可能である。

#### 【0009】

##### <2. 編集スタジオからの盗難>

コンテンツ所有者から発注を受けて編集をする工程においてコンテンツが盗難に会う場合もある。このコンテンツをDVD製造工場へ持ち込むことでROM化されたDVD-Videoを製造することも可能である。

#### 【0010】

##### <3. DVD-Video正規品からの複製（「解読技術」の利用）>

例えば、DVDプレーヤでは、不正なコンテンツ利用を防止する技術としてCSS(Content Scramble System)が採用されている。CSSでは、DVD-ROM(Read Only Memory)に、ビデオデータやオーディオデータ等が暗号化されて記録されており、その暗号化されたデータの復号鍵が、

ライセンスを受けたDVDプレーヤに与えられる。ライセンスは、不正コピーを行わない等の所定の動作規定に従うように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

#### 【0011】

一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するための鍵を有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、CSSの構成では、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

#### 【0012】

しかし、CSSの暗号を破るDeCSSソフトウェアがインターネット上で配布されるという事態が発生している。これは誰でも簡単に入手でき、これを用いて暗号を解いて平文の状態で記録型DVDへ書き込むことが可能である。このようにデジタルビデオディスクへ施された暗号が解読され、このコンテンツをDVD製造工場へ持ち込むことでROM化されたDVD-Videoを製造することも想定される。

#### 【0013】

<4. DVD-Video正規品からの複製（アナログ出力の利用）>

パーソナルコンピュータ（以下、適宜PCと略す）はコンテンツ専用機器ではないことから、コピー制御情報としてコンテンツ格納媒体に記録されている例えばCGMS-A（Copy Generation Management System-Analog）やマクロビジョン信号の反応義務はなく、コピー制限が有効に働かないことから、DVD-Videoプレーヤからの出力をPC内蔵のビデオキャプチャードボードへ入力してHDD（Hard Disc Drive）へコピーすることが可能である。一旦HDDへ記録されたビデオデータは平文の状態で記録型DVDへ書き込むことができる。このコンテンツをDVD製

造工場へ持ち込むことでROM化されたDVD-Videoを製造することも可能である。

【0014】

このように、コピーが違法に行われた記録媒体が市場に流通すると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。

【0015】

なお、コンテンツの不正利用を防止する技術として、本出願人は、例えば特許文献1および特許文献2において、記録媒体に格納するコンテンツのデータブロック毎に異なる鍵を適用した暗号処理技術を提案した。すなわち、データブロック毎の鍵生成情報としてシードを設定し、ブロック毎に設定したシードを暗号鍵の生成に適用する構成により、従来の1つの鍵のみによるコンテンツ暗号化を複雑化して、暗号アルゴリズムの解読困難性を高めたものである。

【0016】

しかし、コンテンツを格納したCD、DVD等の情報記録媒体を製造し販売するプロセスにおいては、様々な外部業者間でコンテンツあるいはコンテンツの暗号化に関連する鍵情報などが流通することになる。

【0017】

しかし、現状においては、コンテンツを格納した情報記録媒体の製造、販売ルートにおけるコンテンツ管理、鍵情報管理を総括的にかつ効率的に実行する適切な構成が実現されているとは言い難く、不正なコピー媒体が市場に流通した場合、その情報漏洩ルートを追跡することは困難となるというのが現状であった。特にコンテンツ編集者自身によるコンテンツの盗難行為やディスク製造者自身による盗難されたコンテンツの製造の結果として市場に流通する媒体は正規品との判別が困難であり、不正な媒体の市場への流通は一層深刻な状況となりつつある。

【0018】

【特許文献1】

特許公開 2 0 0 1 - 3 5 1 3 2 4 号公報

【特許文献2】

特許公開 2002-236622 号公報

【0019】

【発明が解決しようとする課題】

本発明は、上述の従来技術における問題点に鑑みてなされたものであり、DVD、CD等の各種情報記録媒体に格納したコンテンツを再生装置、PC（パーソナルコンピュータ）等の情報処理装置において利用する構成において、コンテンツを格納した情報記録媒体の製造、販売ルートにおいて、管理センタによって管理された正規なエンティティからなる正規のルートを経由していることの確認を可能とし、該確認を条件としてコンテンツの再生を可能としてコンテンツの著作権保護を確実にするとともに、情報記録媒体に格納された各エンティティの識別情報の漏洩防止を実現した情報記録媒体、およびデータ処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0020】

【課題を解決するための手段】

本発明の第1の側面は、

暗号化コンテンツを格納した情報記録媒体であり、

コンテンツと、情報記録媒体の製造ルートのエンティティに対応して設定されたエンティティコードを格納し、一定の暗号処理単位毎に設定した暗号処理鍵生成情報としてのシードに基づいて生成する鍵によって前記暗号処理単位に含まれるデータに暗号化を施した構成を有するとともに、

前記エンティティコードを前記シードの設定領域に重複させることなく、シードに基づいて生成する鍵によって暗号化する暗号化領域に格納した構成を有することを特徴とする情報記録媒体にある。

【0021】

さらに、本発明の情報記録媒体の一実施態様において、前記暗号処理単位は、複数パケットの集合データ領域として設定され、前記シードは、前記暗号処理単位の先頭パケットの先頭データから予め定められたビット数のデータを抽出したデータとして設定される構成であり、前記エンティティコードは、パケット内のペイロードとして格納するとともに、前記シードの構成ビット領域に重複しない

データ領域に格納した構成であることを特徴とする。

【0022】

さらに、本発明の情報記録媒体の一実施態様において、前記エンティティコードはMP E G規格において規定されるプログラムマップテーブル (PMT) に格納され、前記エンティティコードを前記プログラムマップテーブル (PMT) のプログラム情報領域内で、かつプログラムマップテーブル (PMT) を格納する複数の分割パケットの先頭パケットの構成データとしたことを特徴とする。

【0023】

さらに、本発明の情報記録媒体の一実施態様において、前記複数の分割パケットの先頭パケットは183バイトのペイロードを有するトランスポートストリームパケットであり、前記エンティティコードはプログラムマップテーブル (PMT) のプログラム情報領域内で、かつ、プログラムマップテーブル (PMT) の先頭データから183バイト以内のデータとして格納した構成を有することを特徴とする。

【0024】

さらに、本発明の情報記録媒体の一実施態様において、前記エンティティコードはMP E G規格において規定されるプログラムマップテーブル (PMT) に格納され、前記プログラムマップテーブル (PMT) を、複数のトランスポートストリームパケットのペイロードとして分割格納し、該トランスポートストリームパケットにさらにタイムスタンプ情報を設定したソースパケットとして情報記録媒体に分散格納した構成を有することを特徴とする。

【0025】

さらに、本発明の情報記録媒体の一実施態様において、前記情報記録媒体は、前記暗号化処理単位毎に設定された鍵生成情報としての第1シードと、前記第1シードに基づいて生成される第1ブロックキーK b 1に基づいて暗号化された鍵生成情報としての暗号化第2シードと、前記第2シードに基づいて生成される第2ブロックキーK b 2に基づいて暗号化された暗号化コンテンツと暗号化エンティティコードとを含む構成であることを特徴とする。

【0026】

さらに、本発明の情報記録媒体の一実施態様において、前記エンティティコードは、編集スタジオコード（ASC: Authoring Studio Code）と情報記録媒体製造者コード（DMC: Disc Manufacturer Code）を含む構成であることを特徴とする。

#### 【0027】

さらに、本発明の第2の側面は、

情報記録媒体に対する書き込みデータを生成するデータ処理方法であり、

情報記録媒体の製造ルートのエンティティに対応して設定されたエンティティコードの書き込み位置を制御して制御情報テーブル中に設定するエンティティコード設定ステップと、

前記制御情報テーブルを分割格納した複数のパケットを生成するテーブル情報格納パケット生成ステップと、

前記テーブル情報格納パケットをコンテンツ格納パケット列に分散配置するステップと、

一定の暗号処理単位毎に設定した暗号処理鍵生成情報としてのシードに基づいて生成する鍵によって前記暗号処理単位に含まれるデータの暗号化処理を実行するステップとを有し、

前記エンティティコード設定ステップにおいては、

前記エンティティコードを前記シードの設定領域に重複させることなく、シードに基づいて生成する鍵によって暗号化される暗号化領域に含まれるように制御する処理を実行するステップを含むことを特徴とするデータ処理方法にある。

#### 【0028】

さらに、本発明のデータ処理方法の一実施態様において、前記暗号処理単位は、複数パケットの集合データ領域であり、前記シードは前記暗号処理単位の先頭パケットの先頭データから予め定められたビット数のデータであり、前記エンティティコード設定ステップは、前記エンティティコードを、前記シードの構成ビット領域に重複しないデータ領域に設定するステップを含むことを特徴とする。

#### 【0029】

さらに、本発明のデータ処理方法の一実施態様において、前記エンティティコ

ード設定ステップは、MPEG規格において規定されるプログラムマップテーブル（PMT）のプログラム情報領域内で、かつプログラムマップテーブル（PMT）を格納する複数の分割パケットの先頭パケットの構成データとなる位置に、前記エンティティコードを設定する処理を実行することを特徴とする。

#### 【0030】

さらに、本発明のデータ処理方法の一実施態様において、前記複数の分割パケットの先頭パケットは183バイトのペイロードを有するトランスポートストリームパケットであり、前記エンティティコード設定ステップは、前記エンティティコードをプログラムマップテーブル（PMT）のプログラム情報領域内で、かつ、プログラムマップテーブル（PMT）の先頭データから183バイト以内のデータとして設定することを特徴とする。

#### 【0031】

さらに、本発明の第3の側面は、

情報記録媒体に対する書き込みデータを生成する処理を実行するコンピュータ・プログラムであり、

情報記録媒体の製造ルートのエンティティに対応して設定されたエンティティコードの書き込み位置を制御して制御情報テーブル中に設定するエンティティコード設定ステップと、

前記制御情報テーブルを分割格納した複数のパケットを生成するテーブル情報格納パケット生成ステップと、

前記テーブル情報格納パケットをコンテンツ格納パケット列に分散配置するステップと、

一定の暗号処理単位毎に設定した暗号処理鍵生成情報としてのシードに基づいて生成する鍵によって前記暗号処理単位に含まれるデータの暗号化処理を実行するステップとを有し、

前記エンティティコード設定ステップは、

前記エンティティコードを前記シードの設定領域に重複させることなく、シードに基づいて生成する鍵によって暗号化される暗号化領域に含まれるように制御する処理を実行するステップを含むことを特徴とするコンピュータ・プログラム

にある。

### 【0032】

#### 【作用】

本発明においては、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）等のエンティティコードを情報記録媒体に確実に暗号化して格納することが可能となり、外部に対するこれらのエンティティコードの漏洩防止が可能となるので、不正にこれらのエンティティコードを取得して、正規のエンティティになりすました不正コピーコンテンツ格納媒体の製造を防止できる。すなわち、各コードが鍵生成情報としてのシード領域に重ならないようにプログラムマップテーブル（PMT）内でのデータ設定位置を制御する構成としたので、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を格納したプログラムマップテーブルの格納パケットをコンテンツパケット列の任意の位置に設定した場合でも、各エンティティコードが非暗号化データとしてのシード領域に重なることがなく、コードの外部漏洩を防止できる。

### 【0033】

さらに、本発明の構成では、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

### 【0034】

さらに、本発明の構成によれば、各エンティティのコード情報を情報記録媒体に格納する構成としたので、管理センタによって管理されたコンテンツ編集エンティティおよび情報記録媒体製造エンティティのみが正規な暗号化コンテンツを編集し、情報記録媒体を製造することが可能となり、情報記録媒体が不正に複製

された場合には、コード検出による情報漏洩ルートの解析が可能となる。

#### 【0035】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、CDやDVD、MOなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

#### 【0036】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

#### 【0037】

##### 【発明の実施の形態】

以下、本発明の情報記録媒体、およびデータ処理方法、並びにコンピュータ・プログラムの詳細について説明する。

#### 【0038】

##### 〔記録媒体上のデータ記録構成および製造プロセス概要〕

まず、本発明に係る情報記録媒体に格納されるデータ構成および製造プロセス概要について説明する。情報記録媒体に格納された暗号化データは、データ記録再生装置や、PC（パーソナルコンピュータ）において読み取られ、復号、再生される。

#### 【0039】

本発明の情報記録媒体に格納されるデータについて、図1を参照して説明する。図1には、ディスク状の情報記録媒体100を例として示す。なお、本発明における情報記録媒体は、光、磁気、半導体、フラッシュメモリ等、様々な形体の情報記録媒体を含み、ディスク状のものに限定されるものではない。

#### 【0040】

図 1 に示すように、情報記録媒体 1 0 0 には、ディスク ID 1 0 1、物理インデックス 1 0 2、暗号化コンテンツ 1 0 3、記録シード (REC SEED) 1 0 4、暗号鍵情報 1 2 0 が格納される。暗号鍵情報 1 2 0 は、情報記録媒体 1 0 0 のコンテンツ格納領域とは異なる特別のプログラムに基づいて読み取り可能なリードイン領域 1 1 0 に格納される。

#### 【 0 0 4 1 】

暗号鍵情報 1 2 0 には、情報記録媒体 1 0 0 に格納された暗号化コンテンツ 1 0 3 の復号、再生に必要な様々な鍵情報が含まれる。図 1、図 2 を参照して、情報記録媒体に格納される情報の概要と、情報記録媒体の製造ルートについて説明する。

#### 【 0 0 4 2 】

図 2 に示すように、情報記録媒体に格納するコンテンツは、コンテンツ編集エンティティ (A S : Authoring Studio) 3 3 0 において編集され、その後、情報記録媒体製造エンティティ (D M : Disc Manufacturer) 3 5 0 において、ユーザに提供される媒体としての C D、D V D 等が大量に複製 (レプリカ) されて、情報記録媒体 1 0 0 が製造され、ユーザに提供される。情報記録媒体 1 0 0 はユーザの情報処理装置 2 0 0 において再生される。

#### 【 0 0 4 3 】

このディスク製造、販売、使用処理全体についての管理を実行するのが管理センタ (T C : Trusted Center) 3 0 0 である。管理センタ (T C : Trusted Center) 3 0 0 は、コンテンツ編集エンティティ (A S : Authoring Studio) 3 3 0、および情報記録媒体製造エンティティ (D M : Disc Manufacturer) 3 5 0 に対して様々な管理情報を提供し、コンテンツ編集エンティティ (A S : Authoring Studio) 3 3 0、および情報記録媒体製造エンティティ (D M : Disc Manufacturer) 3 5 0 は、管理センタ (T C : Trusted Center) 3 0 0 から受領した管理情報に基づいて、コンテンツの編集、暗号化、鍵情報の、生成、格納処理などを行う。また、管理センタ (T C : Trusted Center) 3 0 0 は、ユーザの情報処理装置に格納するデバイスキーの管理、提供も行う。これらの各情報の詳細については後述する。

## 【0044】

図1に示す暗号鍵情報120には、情報記録媒体100に格納された暗号化コンテンツ103の復号、再生に必要な様々な鍵情報が含まれる。暗号鍵情報120は、管理センタ300が生成し、情報記録媒体製造エンティティ(DM:Disc Manufacturer)350に提供される。情報記録媒体製造エンティティ(DM:Disc Manufacturer)350は、管理センタ300から提供される暗号鍵情報120を情報記録媒体100のリードイン領域110に格納する。

## 【0045】

暗号鍵情報120には、コンテンツ再生に必要なとなるメディアキーKmを暗号化して格納した暗号鍵ブロックとしてのEKB121、コンテンツまたはメディアに対応して設定される第1タイトルキー(Kt1)をメディアキーKmで暗号化した暗号化第1タイトルキーeKm(Kt1)122、第2タイトルキー(Kt2)をメディアキーで暗号化した暗号化第2タイトルキーeKm(Kt2)123、コンテンツ編集エンティティに対応して設定される編集スタジオコード(ASC:Authoring Studio Code)を第2タイトルキー(Kt2)で暗号化した暗号化ASC:eKt2(ASC)124、情報記録媒体製造エンティティに対応して設定される情報記録媒体製造者コード(DMC:Disc Manufacturer Code)を第2タイトルキー(Kt2)で暗号化した暗号化DMC:eKt2(DMC)125を含んでいる。

## 【0046】

なお、編集スタジオコード(ASC)、情報記録媒体製造者コード(DMC)は、コンテンツを格納した情報記録媒体の製造、販売ルートにおいて管理センタが正規のエンティティとして認めた外部業者に対応して設定される識別情報である。本実施例では、それぞれ、編集スタジオの識別子、情報記録媒体製造者識別子として設定したコードデータとした例を説明するが、例えば、記録媒体の製造単位(ロット)毎、発注単位毎の設定コードとしてもよく、あるいは、記録媒体に格納するコンテンツ毎に設定したコードとしてもよい。さらに、コンテンツ格納記録媒体の発注日時、製造日時等の日時情報などを含めたコードとして設定することも可能である。これらのコードデータの格納態様については、後段で詳細

に説明する。

#### 【0047】

EKB121は、有効化キープロック (Enabling Key Block) であり、有効なライセンスを持つユーザの情報処理装置に格納されたデバイスキーに基づく処理(復号)によってのみ、コンテンツの復号に必要なメディアキーを取得する鍵情報ブロックである。これはいわゆる階層型木構造に従った情報配信方式によって、ユーザデバイス(情報処理装置)のライセンスの有効性に基づく鍵取得を可能としたものであり、無効化(リボーク処理)されたユーザデバイスの鍵(メディアキー)取得を阻止可能としたものである。管理センタはEKBに格納する鍵情報の変更により、特定のユーザデバイスに格納されたデバイスキーでは復号できない、すなわちコンテンツ復号に必要なメディアキーを取得できない構成を持つEKBを生成することができる。

#### 【0048】

階層型木構造を適用した暗号鍵等の暗号データ提供処理について、図を参照して説明する。図3の最下段に示すナンバ0～15が、例えばコンテンツ利用を行なう情報処理装置としてのユーザデバイスである。すなわち図3に示す階層ツリー(木)構造の各葉(リーフ：leaf)がそれぞれのデバイスに相当する。

#### 【0049】

各デバイス0～15は、製造時あるいは出荷時、あるいはその後において、図1に示す階層ツリー(木)構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵(ノードキー)および各リーフのリーフキーからなるキーセット(デバイスキー(DNK：Device Node Key))をメモリに格納する。図3の最下段に示すK0000～K1111が各デバイス0～15にそれぞれ割り当てられたリーフキーであり、最上段のKR(ルートキー)から、最下段から2番目の節(ノード)に記載されたキー：KR～K1111をノードキーとする。

#### 【0050】

図3に示す木構造において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRをデバイスキーとして所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15

は、K1111、K111、K11、K1、KRを所有する。なお、図3のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

#### 【0051】

また、図3のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたDVD、CD、MD、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なるデバイス、異なるアプリケーションの共存構成の上に図3に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

#### 【0052】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いる1つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダからネットワークまたはCD等の情報記録媒体に格納して提供したり、各デバイス共通に使用するコンテンツ鍵を送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なうエンティティは、図3の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行可能となる。このようなグループは、図3のツリー中に複数存在する。

#### 【0053】

なお、ノードキー、リーフキーは、ある1つの管理センタ機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグルー

プごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ機能を持つ管理システム、プロバイダ、決済機関等が実行可能である。

#### 【0054】

このツリー構造において、図3から明らかなように、1つのグループに含まれる3つのデバイス0, 1, 2, 3はデバイスキー (DNK: Device Node Key) として共通のキーK00、K0、KRを含むデバイスキー (DNK: Device Node Key) を保有する。このノードキー共有構成を利用することにより、例えば共通のキーをデバイス0, 1, 2, 3のみに提供することが可能となる。たとえば、共通に保有するノードキーK00は、デバイス0, 1, 2, 3に共通する保有キーとなる。また、新たなキーKnewをノードキーK00で暗号化した値Enc (K00, Knew) を、ネットワークを介してあるいは記録媒体に格納してデバイス0, 1, 2, 3に配布すれば、デバイス0, 1, 2, 3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc (K00, Knew) を解いて新たなキーKnewを得ることが可能となる。なお、Enc (Ka, Kb) はKbをKaによって暗号化したデータであることを示す。

#### 【0055】

また、ある時点tにおいて、デバイス3の所有する鍵: K0011, K001, K00, K0, KRが例えば攻撃者 (ハッカー) により解析されて露呈したことが発覚した場合、それ以降、システム (デバイス0, 1, 2, 3のグループ) で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー: K001, K00, K0, KRをそれぞれ新たな鍵K(t)001, K(t)00, K(t)0, K(t)Rに更新し、デバイス0, 1, 2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代 (Generation) : tの更新キーであることを示す。

#### 【0056】

更新キーの配布処理について説明する。キーの更新は、例えば、図4 (A) に示す有効化キーブロック (EKB: Enabling Key Block) と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格

納してデバイス 0, 1, 2 に供給することによって実行される。なお、有効化キーブロック (EKB) は、図 4 に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック (EKB) は、キー更新ブロック (KRB: Key Renewal Block) と呼ばれることもある。

#### 【0057】

図 4 (A) に示す有効化キーブロック (EKB) には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図 4 の例は、図 3 に示すツリー構造中のデバイス 0, 1, 2 において、世代  $t$  の更新ノードキーを配布することを目的として形成されたブロックデータである。図 3 から明らかなように、デバイス 0, デバイス 1 は、更新ノードキーとして  $K(t)00$ 、 $K(t)0$ 、 $K(t)R$  が必要であり、デバイス 2 は、更新ノードキーとして  $K(t)001$ 、 $K(t)00$ 、 $K(t)0$ 、 $K(t)R$  が必要である。

#### 【0058】

図 4 (A) の EKB に示されるように EKB には複数の暗号化キーが含まれる。最下段の暗号化キーは、 $Enc(K0010, K(t)001)$  である。これはデバイス 2 の持つリーフキー  $K0010$  によって暗号化された更新ノードキー  $K(t)001$  であり、デバイス 2 は、自身の持つリーフキーによってこの暗号化キーを復号し、 $K(t)001$  を得ることができる。また、復号により得た  $K(t)001$  を用いて、図 4 (A) の下から 2 段目の暗号化キー  $Enc(K(t)001, K(t)00)$  を復号可能となり、更新ノードキー  $K(t)00$  を得ることができる。以下順次、図 4 (A) の上から 2 段目の暗号化キー  $Enc(K(t)00, K(t)0)$  を復号し、更新ノードキー  $K(t)0$ 、図 4 (A) の上から 1 段目の暗号化キー  $Enc(K(t)0, K(t)R)$  を復号し  $K(t)R$  を得る。

#### 【0059】

一方、デバイス  $K0000$ 、 $K0001$  は、ノードキー  $K000$  は更新する対象に含まれておらず、更新ノードキーとして必要なのは、 $K(t)00$ 、 $K(t)$

0、 $K(t)R$ である。デバイス $K0000$ 、 $K0001$ は、図4(A)の上から3段目の暗号化キー $Enc(K000, K(t)00)$ を復号し $K(t)00$ を取得し、以下、図4(A)の上から2段目の暗号化キー $Enc(K(t)00, K(t)0)$ を復号し、更新ノードキー $K(t)0$ 、図4(A)の上から1段目の暗号化キー $Enc(K(t)0, K(t)R)$ を復号し $K(t)R$ を得る。このようにして、デバイス0、1、2は更新した鍵 $K(t)R$ を得ることができる。なお、図4(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

#### 【0060】

図3に示すツリー構造の上位段のノードキー： $K(t)0$ 、 $K(t)R$ の更新が不要であり、ノードキー $K00$ のみの更新処理が必要である場合には、図4(B)の有効化キーブロック(EKB)を用いることで、更新ノードキー $K(t)00$ をデバイス0、1、2に配布することができる。

#### 【0061】

図4(B)に示すEKBは、例えば特定のグループにおいてのみ取得可能なメディアキー $Km$ を配布する場合に利用可能である。具体例として、図3に点線で示すグループ内のデバイス0、1、2、3にのみ利用可能なメディアキー $Km$ を配布するとする。このとき、デバイス0、1、2、3の共通のノードキー $K00$ を更新した $K(t)00$ を用いて新たなメディアキー $Km$ を暗号化したデータ $Enc(K(t)00, K(t)m)$ を図4(B)に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

#### 【0062】

すなわち、デバイス0、1、2はEKBを処理して得た $K(t)00$ を用いて上記暗号文を復号すれば、 $t$ 時点でのキー、例えばコンテンツの暗号化復号化に適用するメディアキー $K(t)m$ を得ることが可能になる。

#### 【0063】

図5に、 $t$ 時点でのキー、例えばコンテンツの暗号化復号化に適用するメディアキー $K(t)m$ をEKBの処理によって取得する処理例を示す。EKBには、

$K(t)00$ を用いてメディアキー $K(t)m$ を暗号化したデータ $Enc(K(t)00, K(t)m)$ と図4(B)に示すデータとが格納されているとする。ここでは、デバイス0の処理例を示す。

#### 【0064】

図5に示すように、デバイス0は、記録媒体に格納されている世代： $t$ 時点のEKBと自分がかじめ格納しているノードキー $K000$ を用いて上述したと同様のEKB処理により、ノードキー $K(t)00$ を生成する。さらに、復号した更新ノードキー $K(t)00$ を用いて暗号化データ $Enc(K(t)00, K(t)m)$ を復号して更新メディアキー $K(t)m$ を取得する。

#### 【0065】

また、別の例としてツリー構造のノードキーの更新は不必要で、時点 $t$ でのメディアキー $K(t)m$ のみを必要な機器が得られればよいという場合もある。この場合、下記のような方式とすることができる。

#### 【0066】

いま、図3の例と同様にデバイス0, 1, 2にのみメディアキー $K(t)m$ を送りたいとする。このときEKBは、

バージョン (Version) :  $t$

インデックス 暗号化キー

000      $Enc(K000, K(t)m)$

0010    $Enc(K0010, K(t)m)$

となる。

#### 【0067】

デバイス0, 1は $K000$ を用いて、またデバイス2は $K0010$ を用いて上記EKBのうちの1つの暗号文を復号することによりコンテンツ鍵を得ることができる。このようにすることにより、ノードキーの更新は行えないものの必要な機器にコンテンツ鍵を与える方法をより効率よく（すなわち、EKBに含まれる暗号文数を減らしてEKBのサイズを小さくするとともに管理センタでの暗号化およびデバイスでの復号処理の回数を減らせる）することができる。

#### 【0068】

図1に戻り、情報記録媒体100に格納されるその他のデータの詳細について説明する。ディスクID101は、情報記録媒体固有の識別子としての情報記録媒体IDである。管理センタ300が生成して情報記録媒体製造エンティティ350に渡す管理情報であり、ディスク1枚毎に異なるIDである。例えば、管理センタ300はディスク1枚毎に異なるシード(S)を生成し、改竄検証用の電子署名(Sig)を付加したデータ(S, Sig)を管理センタが許容したディスク枚数分生成して情報記録媒体製造エンティティ350に提供する。情報記録媒体製造エンティティ350は、ディスク毎に異なるID情報(S, Sig)を情報記録媒体(ディスク)に格納する。

#### 【0069】

コンテンツ再生を実行するユーザの情報処理装置においては、情報記録媒体(ディスク)に格納されたID情報(S, Sig)を読み取り、署名検証処理によりIDの改竄のないことの確認を条件として、コンテンツ復号プロセスに移行する。なお、署名は公開鍵暗号方式に基づく署名、またはMAC等の共通鍵暗号方式による署名等の利用が可能である。公開鍵暗号方式に基づく署名を適用する場合は、管理センタ300は、秘密鍵による署名生成を実行し、各ユーザの情報処理装置では、管理センタ300の公開鍵による署名検証を実行する。共通鍵方式の場合は、管理センタ、ユーザデバイス双方において共通の署名用鍵を保有し、署名生成、検証処理を実行する。ユーザの情報処理装置(ユーザデバイス)における処理については後述する。

#### 【0070】

図1に示す情報記録媒体に格納される物理インデックス102は、情報記録媒体製造エンティティ350が生成して、情報記録媒体に格納する。記録シード(REC SEED)104は、コンテンツ編集エンティティ330が生成して、情報記録媒体製造エンティティ350に渡されて情報記録媒体に格納する値である。

#### 【0071】

暗号化コンテンツ103には、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)とを含むプログラムマップテーブルPMT(Program Ma

p Table)が格納される。PMTは編集スタジオコード(ASC)と、情報記録媒体製造者コード(DMC)を含む情報であり、コンテンツ編集エンティティ330においてコンテンツに対して埋め込まれる。さらに、暗号化コンテンツ103には電子透かし(WM:Water Mark)情報としての編集スタジオコード(ASC:Authoring Studio Code)と、情報記録媒体製造者コード(DMC:Disc Manufacturer Code)が格納される。これらのコード埋め込みは、管理センタ300において行われる。情報記録媒体に対する様々なデータ埋め込み処理の詳細なシーケンスについては後述する。

#### 【0072】

情報記録媒体に格納される暗号化コンテンツは、例えばMP EG-2システムで規定されている符号化データとしてのトランスポートストリーム(TS)として構成される。トランスポートストリームは、1本のストリームの中に複数のプログラムを構成することができ、各トランスポートパケットの出現タイミング情報としてのATS(Arrival Time Stamp:着信時刻スタンプ)が設定されている。このタイムスタンプは、MP EG-2システムで規定されている仮想的なデコーダであるTSTD(Transport Stream System Target Decoder)を破綻させないように符号化時に決定され、ストリームの再生時に、各トランスポートパケットに付加されたATSによって出現タイミングを制御して、復号、再生を行う。

#### 【0073】

例えば、トランスポートストリームパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

#### 【0074】

図6を参照して、情報記録媒体に格納されるデータ記録構成および、記録データの復号再生処理の概要を説明する。情報記録媒体に格納されるデータは暗号化データであり、再生を行う場合には、復号処理を行うことが必要となる。図6(a)が情報記録媒体に格納されるデータ記録構成である。18バイトの制御デー

タ (User Control Data) と、2048 バイトのユーザデータ (User Data) が 1 つのセクタデータとして構成され、例えば 3 セクタ分のデータが 1 つの暗号処理単位として規定される。なおここで説明するバイト数や、処理単位は 1 つの代表例であり、制御データ、ユーザデータのバイト数や、処理単位の設定は、様々な設定が可能である。

#### 【0075】

(b) は、暗号処理単位である 1 ユニット (1 AU: Aligned Unit) の構成を示す。情報記録媒体に格納された暗号化データの再生を実行する情報処理装置は、制御データ内のフラグに基づいて、暗号処理単位である 1 AU (Aligned Unit) を抽出する。

#### 【0076】

暗号処理単位である 1 ユニット (1 AU) には、(c) 暗号化構成に示すように、ブロックキー K b 1 によって暗号化された領域、ブロックキー K b 2 によって暗号化された領域が含まれる。ブロックキー K b 1 と K b 2 によって二重に暗号化された領域を含める構成としてもよい。ブロックキーを生成するためには、鍵生成情報としてのシード情報が必要となる。シード情報 (シード 1) はブロックキー K b 1 を生成するための鍵生成情報であり、シード情報 (シード 2) はブロックキー K b 2 を生成するための鍵生成情報であり、各暗号処理単位 (1 AU) 毎に、暗号処理単位内の格納情報、すなわち制御情報やユーザデータ領域のコンテンツ等のデータ列から抽出した例えば 128 ビットあるいは 64 ビット情報が用いられる。図 6 (c) に示すシード情報の格納態様、暗号化態様は一例であり、後段において、複数の構成例について説明する。

#### 【0077】

ユーザデータ領域に格納された暗号化コンテンツを復号するためには、情報記録媒体に格納されたシード情報を読み取って、シード情報に基づく鍵 (ブロック鍵) を生成して生成したブロック鍵を用いた復号処理を実行することが必要となる。

#### 【0078】

図 6 (c) に示すように、ブロックキー K b 1 を生成するために必要となるシ

ード情報（シード1）と、ブロックキーKb2を生成するために必要となるシード情報（シード2）とを情報記録媒体上に格納するとともに、一方のシード情報（シード2）をシード情報（シード1）によって生成されるブロックキーKb1によって暗号化して格納している。また、暗号化コンテンツ中に、編集スタジオコード（ASC）と、情報記録媒体製造者コード（DMC）を含むプログラムマップテーブルPMT（Program Map Table）が格納される。さらに、電子透かし（WM：Water Mark）としても、コンテンツ編集スタジオコード（ASC：Authoring Studio Code）、情報記録媒体製造者コード（DMC：Disc Manufacturer Code）が格納される。

#### 【0079】

このように、2つの異なる鍵を適用した暗号化処理を実行したデータを記録媒体に格納し、再生処理において2つの異なる鍵を適用した復号処理を行う。すなわち、所定の暗号処理単位毎に異なる鍵生成情報であるシード1、シード2を適用した暗号処理によりブロックキーKb1、Kb2を生成して復号処理を実行する。

#### 【0080】

1処理単位毎の復号処理の後、復号されたトランスポートストリームパッケージがMP EG-2デコーダに入力されデコード処理が実行されてコンテンツ再生が行なわれる。1つの処理単位（3セクタ）には、例えば32個のトランスポートストリーム（TS）パッケージが含まれる。すなわち、 $32 \times 192 = 6144$ バイトデータが1つの暗号化および復号処理単位とされる。なお、処理単位の設定は、様々な設定が可能である。

#### 【0081】

復号再生時には、各処理単位毎に2つのシード情報（シード1、シード2）を情報記録媒体から取得し、各シード情報に基づいて2つのブロックキーKb1、Kb2を生成し、生成したブロックキーKb1、Kb2を用いて復号処理がなされて、コンテンツ再生が行われる。

#### 【0082】

また、コンテンツの記録時には、復号再生処理と逆のプロセスが実行され、各

処理単位毎に2つのシード情報（シード1、シード2）を設定し、各シード情報に基づいて2つのブロックキーKb1、Kb2を生成し生成したブロックキーKb1、Kb2を用いて暗号化処理がなされて、コンテンツ記録が行われる。

#### 【0083】

また、前述したように、DVD等のコンテンツ記録媒体には、暗号化コンテンツとともに、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）とを含むプログラムマップテーブルPMT（Program Map Table）が格納される。これらのコードを含むプログラムマップテーブルPMTは、コンテンツ編集エンティティ330（図2参照）においてコンテンツに対して埋め込まれる。

#### 【0084】

編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を含むプログラムマップテーブルPMTの埋め込み態様について説明する。なお、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）は、前述したように、編集スタジオの識別子、情報記録媒体製造者識別子として設定したコードデータとするのみならず、記録媒体の製造単位（ロット）毎、発注単位毎の設定コードとしてもよく、あるいは、記録媒体に格納するコンテンツ毎に設定したコードとしてもよい。さらに、コンテンツ格納記録媒体の発注日時、製造日時等の日時情報などを含めたコードとして設定することも可能である。

#### 【0085】

また、本実施例では、識別コードとして編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）の適用例について説明するが、管理センタの管理するエンティティ、例えばコンテンツ記録媒体の製造、流通過程に存在する様々なエンティティに対応して識別情報（コード）を付与する構成が可能であり、これらの各エンティティに付与される識別コードに基づく管理が可能となる。以下では、管理センタの管理するエンティティが編集スタジオと情報記録媒体製造者であり、これらのエンティティに対応する識別コードとして編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を設定した管理構成例について説明する。

#### 【0086】

編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) を含むプログラムマップテーブルPMTデータのコンテンツに対する挿入例を図7に示す。図7 (a) に示すプログラムマップテーブル (PMT) は、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) 以外にも様々な制御情報、識別情報を含む情報として設定され、そのデータ長は任意であり、可変長データである。

#### 【0087】

このプログラムマップテーブル (PMT) は、図7 (b) に示すように、そのデータ長に応じた任意の数の複数のTSパケット (188バイト) のペイロード部に分割されて格納され、4バイトのTSパケットヘッダが設定される。プログラムマップテーブル (PMT) の分割データを格納したTSパケットは、さらに図7 (c) に示すように、タイムスタンプ情報やコピー制御情報 (CCI: Copy Control Information) からなるヘッダ情報 (4バイト) が付加されてソースパケット (192バイト) 形式として設定される。

#### 【0088】

記録媒体に格納される暗号化コンテンツ自体も多数のソースパケットによって構成されており、プログラムマップテーブル (PMT) データ格納ソースパケット (PMTパケット) は、図7 (d) に示すように暗号化コンテンツ格納ソースパケットの中に分散して配置される。コンテンツパケット中の個々のPMTパケットの配置位置は規定されておらず、任意の位置に配置することが可能である。

#### 【0089】

ただし、プログラムマップテーブル (PMT) データ全体が、一定のコンテンツ再生期間 (例えば0.1秒) において読み取り可能とするように格納することが必要であり、図7 (e) に示すように、複数のパケットに分割されてコンテンツソースパケット列に分散配置されたプログラムマップテーブル (PMT) のデータ全体が、一定のコンテンツ再生期間 (例えば0.1秒) 毎に繰り返し読み取り可能なようにコンテンツ中に配置される。

#### 【0090】

図7 (d) に示すように、32個のソースパケットを集めたものが、暗号処理

単位である 6 1 4 4 バイトの 1 ユニット (1 A U : A l i g n e d U n i t) であり、図 6 を参照して説明した構成を持つ。I S O / I E C 1 3 8 1 8 - 1 : 1 9 9 6 (M P E G システム) で規定されているトランスポートストリーム形式を使用してコンテンツを記録する場合、上述したプログラムマップテーブル (P M T : P r o g r a m M a p T a b l e) を記録することが必要とされる。P M T は P A T (P r o g r a m A s s o c i a t i o n T a b l e) によって指定される P I D を持った T S パケットに記録される。

#### 【0 0 9 1】

ただし、従来のプログラムマップテーブル (P M T) では、本明細書において説明する編集スタジオコード (A S C) や情報記録媒体製造者コード (D M C) についての記録については定めていない。編集スタジオにおいて実行する編集スタジオコード (A S C) と、情報記録媒体製造者コード (D M C) の埋め込み処理の詳細については、後段で詳細に説明する。

#### 【0 0 9 2】

##### [情報処理装置構成]

図 8 は、上述した暗号化コンテンツ態様を持つコンテンツの記録再生処理を実行する情報処理装置 2 0 0 の一実施例構成を示すブロック図である。情報処理装置 2 0 0 は、入出力 I / F (I n t e r f a c e) 2 2 0、M P E G (M o v i n g P i c t u r e E x p e r t s G r o u p) コーデック 2 3 0、A / D、D / A コンバータ 2 4 1 を備えた入出力 I / F (I n t e r f a c e) 2 4 0、暗号処理手段 2 5 0、再生制御処理手段 2 5 5、R O M (R e a d O n l y M e m o r y) 2 6 0、C P U (C e n t r a l P r o c e s s i n g U n i t) 2 7 0、メモリ 2 8 0、記録媒体 2 9 5 のドライブ 2 9 0、さらにトランスポートストリーム処理手段 (T S 処理手段) 2 9 8 を有し、これらはバス 2 1 0 によって相互に接続されている。

#### 【0 0 9 3】

入出力 I / F 2 2 0 は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス 2 1 0 上に出力するとともに、バス 2 1 0 上のデジタル信号を受信し、外部に出力する。M P E G コーデック 2 3 0 は、バス 2 1 0 を介して供給される M P E G 符号化されたデータを、M P

E G デコードし、入出力 I / F 2 4 0 に出力するとともに、入出力 I / F 2 4 0 から供給されるデジタル信号を M P E G エンコードしてバス 2 1 0 上に出力する。入出力 I / F 2 4 0 は、A / D, D / A コンバータ 2 4 1 を内蔵している。入出力 I / F 2 4 0 は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A / D, D / A コンバータ 2 4 1 で A / D (Analog to Digital) 変換することで、デジタル信号として、M P E G コーデック 2 3 0 に出力するとともに、M P E G コーデック 2 3 0 からのデジタル信号を、A / D, D / A コンバータ 2 4 1 で D / A (Digital to Analog) 変換することで、アナログ信号として、外部に出力する。

#### 【 0 0 9 4 】

暗号処理手段 2 5 0 は、例えば、1 チップの L S I (Large Scale Integrated Circuit) で構成され、バス 2 1 0 を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス 2 1 0 上に出力する構成を持つ。再生制御処理手段 2 5 5 は、コンテンツ再生において検証すべき各種処理を実行して、再生条件を満足しない場合には、コンテンツ再生の停止を行う。暗号処理手段 2 5 0 および再生制御処理手段 2 5 5 の処理の詳細については後述する。

#### 【 0 0 9 5 】

なお、暗号処理手段 2 5 0 は 1 チップ L S I に限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。図においては、暗号処理手段 2 5 0、再生制御処理手段 2 5 5 をそれぞれ個別のブロックとして示してあるが、これらはたとえば C P U 2 7 0 の制御の下に実行するプログラムに基づいて実行する処理とすることも可能である。

#### 【 0 0 9 6 】

R O M 2 6 0 は、例えば、情報処理装置ごとに固有の、あるいは、複数の情報処理装置のグループごとに固有のデバイスキーや、相互認証時に必要とする認証キーを記憶している。デバイスキーは、例えば鍵配信ツリー構成に基づいて提供される暗号化鍵ブロック情報としての E K B (Enabling Key Block) を復号してメディアキーを取得するために用いられる。すなわち、デバイスキーは、メディアキー生成情報として適用される。

## 【0097】

CPU270は、メモリ280に記憶されたプログラムを実行することで、MPEGコーデック230や暗号処理手段250等を制御する。メモリ280は、例えば、不揮発性メモリで、CPU270が実行するプログラムや、CPU270の動作上必要なデータを記憶する。メモリ280が不揮発性メモリの場合、デバイスキーを記憶することも可能であり、以降の実施例ではデバイスキーはメモリ280へ格納するとして説明をする。ドライブ290は、デジタルデータを記録再生可能な記録媒体295を駆動することにより、記録媒体295からデジタルデータを読み出し（再生し）、バス210上に出力するとともに、バス210を介して供給されるデジタルデータを、記録媒体295に供給して記録させる。

## 【0098】

記録媒体295は、例えば、DVD、CD等の光ディスク、光磁気ディスク、磁気ディスク、磁気テープ、あるいはフラッシュROM、MRAM、RAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、図1を参照して説明した各種データを格納した情報記録媒体である。本実施の形態では、ドライブ290に対して着脱可能な構成であるとする。但し、記録媒体295は、情報処理装置200に内蔵する構成としてもよい。

## 【0099】

トランスポートストリーム処理手段（TS処理手段）298は、複数のコンテンツが多重化されたトランスポートストリームから特定のコンテンツに対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体295に格納するためのデータ処理を実行し、また、記録媒体295からの暗号化コンテンツの復号再生時には、トランスポートストリームの出現タイミング制御を行なう。

## 【0100】

トランスポートストリームには、前述したように、各トランスポートパケットの出現タイミング情報としてのATS（Arrival Time Stamp：着信時刻スタンプ）が設定されており、MPEG2デコーダによる復号時にATSによってタイミング制御を実行する。トランスポートストリーム処理手段（TS処理手段）29

8は、例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。

#### 【0101】

本発明の情報処理装置200は、例えば上述のトランスポートストリームによって構成される暗号化コンテンツの記録再生を実行する。これらの処理の詳細については、後段で説明する。なお、図8に示す暗号処理手段250、TS処理手段298は、理解を容易にするため、別ブロックとして示してあるが、両機能を実行する1つのワンチップLSIとして構成してもよく、また、両機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。さらには、ドライブ290、記録媒体295を除く全てのブロックをワンチップLSIとして構成してもよく、また、これらの機能をソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよく、これにより情報処理装置200の改造によるセキュリティ機能の無効化に対するロバストネスを向上させることが出来る。

#### 【0102】

##### [データ再生処理]

次に、記録媒体に格納された暗号化データの復号処理および再生制御処理について説明する。図9に示すように、情報処理装置200におけるコンテンツ再生は、暗号処理手段250における暗号化コンテンツの復号処理と、再生制御手段255における再生制御処理の2つのステップを含む。

#### 【0103】

情報記録媒体100から各種の情報が読み取られ、暗号処理手段250における暗号化コンテンツの復号処理が実行され、復号コンテンツが再生制御手段255に渡され、再生条件判定処理が実行され、再生条件を満足する場合にのみコンテンツ再生が継続して実行され、再生条件を満足しない場合には、コンテンツ再生が停止される。

#### 【0104】

まず、暗号処理手段250における暗号化コンテンツの復号処理の詳細について、図10以下を参照して説明する。

#### 【0105】

コンテンツ復号プロセスでは、まず、暗号処理手段250は、メモリに格納しているデバイスキー410を読み出す。デバイスキー410は、コンテンツ利用に関するライセンスを受けた情報処理装置に格納された秘密キーである。

#### 【0106】

次に、暗号処理手段250は、ステップS11において、デバイスキー410を適用して情報記録媒体100に格納されたメディアキー格納EKBの復号処理を実行して、メディアキーKmを取得する。

#### 【0107】

次に、ステップS12において、情報記録媒体100に格納されたメディアキーKmにより暗号化された暗号化第2タイトルキーeKm(Kt2)を、ステップS11におけるEKB処理で取得したメディアキーKmを用いて復号し、第2タイトルキーKt2を取得する。第2タイトルキーKt2は、再生制御処理手段255に出力される。

#### 【0108】

ステップS13において、情報記録媒体100に格納されたメディアキーKmにより暗号化された暗号化第1タイトルキーeKm(Kt1)を、ステップS11におけるEKB処理で取得したメディアキーKmを用いて復号し、第1タイトルキーKt1を取得する。

#### 【0109】

次にステップS14で、情報記録媒体100に格納されたディスクIDからディスク固有シード(S)を取得する。暗号処理手段250は、情報記録媒体100に格納された識別情報としてのディスクID(Disc ID)404を読み出して、ディスクID404の検証処理を実行する。ディスクIDは、管理センタ300が生成したディスク1枚毎に異なるシードSと改竄検証用の電子署名(Sig)を持つデータ(S, Sig)である。暗号処理手段250は、情報記録媒体100に格納されたID情報(S, Sig)を読み取り、署名検証処理によりID

の改竄のないことを確認する。公開鍵暗号方式に基づく署名の場合は、管理センタ 300 の公開鍵による署名検証を実行する。共通鍵方式の場合は、共通鍵により署名検証処理を実行する。署名検証処理により ID の改竄のないことの確認を条件として、ステップ S 14 で、情報記録媒体 100 に格納されたディスク ID からディスク固有シード S を取得する。署名検証処理により ID の改竄があると判定した場合は、コンテンツ復号処理は停止する。

#### 【0110】

署名検証処理により ID の改竄のないことの確認がなされると、次に、ステップ S 15 において、ディスク固有シード S と、タイトルキー K 2 を用いて、ディスク固有キー (Disc Unique Key) K d を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、例えば、図 11 (a) に示すように、ディスク固有シード S を入力値とし、共通鍵暗号方式である AES (Advanced Encryption Standard) 暗号を、タイトルキー K 2 を暗号鍵として実行する方法や、図 11 (b) に示すように、FIPS 180-1 で定められているハッシュ関数 SHA-1 に、タイトルキー K 2 とディスク固有シード S とのビット連結により生成されるデータを入力し、その出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用方法などが適用できる。

#### 【0111】

さらに、暗号処理手段 250 は、ステップ S 13 において生成した第 1 タイトルキー K t 1 と、情報記録媒体 100 から読み出した物理インデックス 406 とに基づいて、ステップ S 16 において、第 1 記録キー (REC キー) K 1 を生成し、また、ステップ S 15 において生成したディスク固有キー K d と、情報記録媒体 100 から読み出した記録シード (REC SEED) 405 とに基づいて、ステップ S 17 において、第 2 記録キー (REC キー) K 2 を生成する。これらの各キーの生成処理においても AES 暗号処理等、ハッシュ関数、縮約関数などが適宜使用される。

#### 【0112】

記録キー K 1、K 2 は、上述の再生処理プロセスにおいて使用することが必要となるが、コンテンツを情報記録媒体に記録する暗号処理においても適用される

鍵、記録処理については後述する。

#### 【0113】

ステップS16、S17において2つの記録キー（RECキー）1，2を生成すると、次に、ステップS18から、情報記録媒体100に格納された暗号化コンテンツ407の読み出しおよび2つのブロックキーKb1，Kb2による復号処理が開始される。

#### 【0114】

ステップS18において、情報記録媒体100に格納された暗号化コンテンツ407から制御情報（UCD：User Control Data）に含まれるシード情報（シード1）が取得され、ステップS19において、シード情報（シード1）と、ステップS16において生成した第1記録キーK1とに基づく暗号処理を実行してブロックキーKb1を生成する。

#### 【0115】

ステップS19のブロックキーKb1の生成処理以降に実行する処理について、図10とともに図12を参照して説明する。

#### 【0116】

図12において、復号処理は、処理単位420を単位として実行される。この処理単位は、先に図6を参照して説明した（b）処理単位に相当する。すなわち、暗号処理単位である1ユニット（1AU：Aligned Unit）である。情報記録媒体100に格納された暗号化データの再生を実行する暗号処理手段250は、制御データ内のフラグに基づいて、暗号処理単位である1AU（Aligned Unit）を抽出する。

#### 【0117】

処理単位420には、18バイトの制御データ（UCD：User Control Data）421と、6144バイトのユーザデータ（暗号化コンテンツを含む）が含まれる。6144バイトのユーザデータは、トランスポートストリームパケットの単位である192バイト毎に分割される。ユーザデータの先頭のTSパケット422と、後続の5952バイトのTSパケット群423を分離して説明する。この例では、シード情報（シード1）431が制御データ421に格納され、シー

ド情報（シード2）432がユーザデータ内の先頭のTSパケット422内に暗号化されて格納された例である。

#### 【0118】

なお、シード情報としての、シード1、シード2の格納態様には複数の態様があり、ここではその一例を示す。他の例については、後段で説明する。

#### 【0119】

図12において、図10の処理ステップと同様の処理ステップには、同一の処理ステップ番号を付してある。

#### 【0120】

ステップS19（図10、図12）においては、情報記録媒体の制御データ内から読み出したシード情報（シード1）431をAES暗号処理部に入力し、先のステップS16において生成した記録キーK1を適用したAES暗号処理を実行しブロックキーKb1を生成する処理を実行する。なお、図12においてAES\_\_Gは、AES暗号処理を適用した鍵生成（Key Generation）処理を示し、AES\_\_Dは、AES暗号処理を適用したデータ復号（Decryption）処理を示している。

#### 【0121】

ステップS20（図10、図12参照）では、ステップS19において生成したブロックキーKb1を適用したAES復号処理を実行する。ステップS20では、ブロックキーKb1を適用した暗号処理のなされたデータ部のみを対象とした復号処理が実行される。この例では、ユーザデータの先頭TSパケット422の少なくともシード情報（シード2）を含むデータ領域がブロックキーKb1を適用した暗号処理のなされたデータ部である。従って、このシード情報（シード2）を含むデータ領域を対象としてブロックキーKb1を適用した復号処理を実行する。

#### 【0122】

なお、ブロックキーKb1を適用した暗号処理のなされたデータ部をどのデータ領域とするかについては、いくつかのパターンがあり、これらについては後述する。

## 【0123】

先頭TSパケット422には、他のユーザデータ部、すなわち、後続の5952バイトのTSパケット群423の復号処理に適用するブロックキーKb2を算出するために必要となるシード情報（シード2）432が含まれている。すなわち、シード情報（シード2）432は、ブロックキーKb1を適用した暗号処理がなされた暗号化データとして先頭TSパケット422に記録されている。

## 【0124】

ステップS20における、ブロックキーKb1を適用した復号処理の結果として、復号TSパケット424が算出され、その中からシード情報（シード2）を抽出する。

## 【0125】

図10のセレクトステップS21は、ブロックキーKb1を適用した復号処理の結果から、シード情報（シード2）をステップS22のブロックキーKb2生成ステップに出力し、ブロックキーKb2で暗号化された暗号化データを復号ステップS23に出力し、その他の復号データ（非暗号化データ）をセレクトステップS24に出力することを示している。

## 【0126】

ステップS22（図10、図12参照）では、ステップS20におけるブロックキーKb1を適用した復号処理の結果取得された復号TSパケット424から抽出したシード情報（シード2）と、ステップS17（図10参照）において生成した記録キーK2とに基づいて、AES暗号処理を実行し、ブロックキーKb2を算出する。

## 【0127】

次に、ステップS23において、ブロックキーKb2を適用してユーザデータ部の暗号化部（ブロックキーKb2で暗号化されたデータ領域423）を復号し、復号TSパケット群425を生成する。

## 【0128】

復号TSパケット群425、および復号TSパケット426（＝TSパケット424）は、セレクトステップS24において結合されて、復号TSパケットか

らなるコンテンツ 412 として再生制御処理手段 255 に入力される。

【0129】

再生制御処理手段 255 における再生制御処理について、図 13 を参照して説明する。再生制御処理手段 255 は、暗号処理手段 250 から、第 2 タイトルキー (Kt2) , 411 と、復号コンテンツ 412 を受領する。

【0130】

まず、再生制御処理手段 255 は、ステップ S31 において、情報記録媒体 100 に格納された暗号化 ASC すなわち、第 2 タイトルキー (Kt2) で暗号化した編集スタジオコード (ASC: Authoring Studio Code) であるデータ eKt2 (ASC) を読み出し、暗号処理手段 250 から受信した第 2 タイトルキー (Kt2) を適用して復号処理を実行し、編集スタジオコード (ASC) を取得しメモリに格納する。

【0131】

さらに、再生制御処理手段 255 は、ステップ S32 において、情報記録媒体 100 に格納された暗号化 DMC すなわち、第 2 タイトルキー (Kt2) で暗号化した情報記録媒体製造者コード (DMC: Disc Manufacturer Code) であるデータ eKt2 (DMC) を読み出し、暗号処理手段 250 から受信した第 2 タイトルキー (Kt2) を適用して復号処理を実行し、情報記録媒体製造者コード (DMC) を取得しメモリに格納する。

【0132】

再生制御処理手段 255 は、暗号処理手段 250 から受信した復号コンテンツ 412 から、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) とを含むプログラムマップテーブル PMT (Program Map Table) を検出する。PMT は編集スタジオコード (ASC) と、情報記録媒体製造者コード (DMC) を含む情報であり、コンテンツ編集エンティティ 330 においてコンテンツに対して埋め込まれる。ステップ S33 において編集スタジオコード (ASC) 検出、ステップ S34 において情報記録媒体製造者コード (DMC) 検出を実行する。

【0133】

ステップS35において、PMTから検出した編集スタジオコード(ASC)と、ステップS31で、暗号化編集スタジオコードeKt2(ASC)の復号処理によって取得しメモリに格納した編集スタジオコード(ASC)との比較処理を実行する。

#### 【0134】

さらに、ステップS36において、PMTから検出した情報記録媒体製造者コード(DMC)と、ステップS32で、暗号化情報記録媒体製造者コード(DMC)eKt2(DMC)の復号処理によって取得しメモリに格納した情報記録媒体製造者コード(DMC)との比較処理を実行する。

#### 【0135】

さらに、ステップS37において、コンテンツ412中から、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を含む電子透かしが規定時間内に検出され、電子透かし格納情報と、メモリ格納情報とが一致したか否かを判定する。再生制御処理手段255では、コンテンツの再生開始からタイマを設定し、予め定めた定時間内に編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を含む電子透かしが検出されたか否かを判定する。

#### 【0136】

ステップS38において、ステップS35における比較結果の一致、すなわち、PMTから検出した編集スタジオコード(ASC)と、メモリに格納した編集スタジオコード(ASC)との一致、ステップS36における比較結果の一致、すなわち、PMTから検出した情報記録媒体製造者コード(DMC)と、メモリに格納した情報記録媒体製造者コード(DMC)との一致、さらに、ステップS37における規定時間内の電子透かし検出、照合のすべてを満足したか否かを判定する。

#### 【0137】

ステップS39において、ステップS38の判定がYesであればコンテンツ再生を継続し、Noであれば、コンテンツ再生を停止する。

#### 【0138】

図14、図15を参照してコンテンツ再生を実行するユーザデバイスとしての

情報処理装置におけるコンテンツ再生処理手順の一連の処理について説明する。

【0139】

ステップS101において、情報処理装置（ユーザデバイス）は、情報記録媒体から暗号鍵情報および識別情報の読み取りを実行する。ステップS102において、読み取り情報および自デバイスに格納したデバイスキーに基づいてタイトルキー（ $K_{t1}$ 、 $K_{t2}$ ）を生成する。

【0140】

ステップS103において、情報記録媒体からディスクID（ $S$ 、 $S_{ig}$ ）を読み取り、検証処理を実行する。検証が成立しない場合は、この時点でコンテンツ再生は停止する。検証が成立すると、ステップS105において、記録キー $K_1$ 、 $K_2$ を生成する。

【0141】

ステップS106において、第2タイトルキー（ $K_{t2}$ ）に基づいて情報記録媒体から読み出した暗号化ASC、暗号化DMC、すなわち、 $eK_{t2}(ASC)$ 、 $eK_{t2}(DMC)$ の復号処理を実行して、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）をメモリに格納する。

【0142】

ステップS107において、ブロックキー $K_{b1}$ 、 $K_{b2}$ を生成し、生成したブロックキー $K_{b1}$ 、 $K_{b2}$ に基づくコンテンツの復号、再生処理を開始する。

【0143】

ステップS108では、コンテンツ再生を実行しながらPMTおよび電子透かしの検出処理を実行する。ステップS109においてPMTから編集スタジオコード（ASC）が検出されるとステップS110において検出した編集スタジオコード（ASC）と、メモリに格納済みの編集スタジオコード（ASC）との比較処理を実行し、一致しなかった場合は、ステップS121でコンテンツ再生を停止する。

【0144】

一致した場合は、さらに、ステップS111に進み、PMTから情報記録媒体製造者コード（DMC）が検出されると、ステップS112において検出した情

報記録媒体製造者コード (DMC) と、メモリに格納済みの情報記録媒体製造者コード (DMC) との比較処理を実行し、一致しなかった場合は、ステップ S 1 2 1 でコンテンツ再生を停止する。

【0145】

一致した場合は、さらに、ステップ S 1 1 3 に進み、電子透かし情報から編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) が検出されると、ステップ S 1 1 4 において検出した編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) と、メモリに格納済みの編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) との比較処理を実行し、一致しなかった場合は、ステップ S 1 2 1 でコンテンツ再生を停止する。

【0146】

ステップ S 1 1 5 では、予め定めた時間内に、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) との PMT と電子透かし情報が検出されたか否かが判定され、検出されなかった場合は、ステップ S 1 2 1 でコンテンツ再生を停止する。

【0147】

編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) との PMT、電子透かし情報との検出処理は規定時間毎に繰り返し実行する。先に図 7 を参照して説明したように、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) とを含む PMT は一定の読み取り期間 (例えば 0.1 秒再生期間) ごとに繰り返し記録されており、再生機は、これらの情報を繰り返し、読み取り、比較処理を実行する。電子透かしも同様である。従って、コンテンツ途中からの再生処理においても、PMT および電子透かしに基づく編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) の検証が確実に実行されることになる。

【0148】

ただし、1 つの編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) との PMT、電子透かし情報との検出がなされ、両者がメモリ格納情報と一致した場合は、その後のコード検証処理を省略する構成としてもよい。

## 【0149】

上述したように、情報記録媒体に格納されたコンテンツは、シード情報（シード1）およびシード情報（シード2）によって生成されるブロック鍵 $Kb1$ 、 $Kb2$ で暗号化され、シード情報（シード2）は、シード情報（シード1）を用いて生成される鍵、すなわちブロックキー $Kb1$ によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報（シード2）の解析、シード情報（シード2）を適用して生成するブロックキー $Kb2$ の解析、ブロックキー $Kb2$ によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

## 【0150】

さらに、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

## 【0151】

次に、図16を参照してシード情報（シード1）と記録キー $K$ に基づいて生成するブロックキー $Kb1$ によって暗号化する領域の例について説明する。図16は、制御ブロックにシード情報（シード1）が格納され、シード情報（シード2）が、ユーザデータの1つのTSパケットに含まれる場合の例である。先に図12を参照して説明したように、シード情報（シード2）は、例えば128ビットデータであり、1つの暗号処理単位（1AU）の先頭のパケットの先頭部に含まれる情報が適用される。

## 【0152】

パケットにシード情報（シード2）を格納した場合、シード情報（シード1）

と記録キー K 1 とに基づいて生成するブロックキー K b 1 によって暗号化する領域例として、例えば図 1 6 (a) ~ (c) の構成がある。(a) は、シード情報 (シード 2) のみをブロックキー K b 1 によって暗号化した例である。それ以外の領域は、非暗号化領域とするか、あるいは、シード情報 (シード 2) と記録キー K 2 によって生成されるブロックキー K b 2 によって暗号化したデータ領域とする。

#### 【0 1 5 3】

(b) は、シード情報 (シード 2) を含む T S パケットの一部領域をブロックキー K b 1 によって暗号化した例である。

#### 【0 1 5 4】

(c) は、シード情報 (シード 2) を含む 1 つの T S パケットの全領域をブロックキー K b 1 によって暗号化した例である。

#### 【0 1 5 5】

このように、シード情報 (シード 1) およびシード情報 (シード 2) の格納態様、および暗号化データ領域の設定態様は様々な設定が可能である。しかし、いずれの場合もシード情報 (シード 2) は、シード情報 (シード 1) を用いて生成される鍵、すなわちブロックキー K b 1 によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報 (シード 2) の解析、シード情報 (シード 2) を適用して生成するブロックキー K b 2 の解析、ブロックキー K b 2 によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

#### 【0 1 5 6】

[情報記録媒体に対するデータ格納処理]

先に図 2 を参照して説明したように、暗号化コンテンツを格納した情報記録媒体は、コンテンツ編集エンティティ (A S : Authoring Studio) 3 3 0 において編集され、その後、情報記録媒体製造エンティティ (D M : Disc Manufacturer) 3 5 0 において、ユーザに提供される媒体としての C D、D V D 等が大量に複製 (レプリカ) されて、情報記録媒体 1 0 0 が製造され、ユーザに提供される。

#### 【0 1 5 7】

このディスク製造、販売、使用処理全体についての管理を実行するのが管理センタ (TC:Trusted Center) 3 0 0 である。管理センタ (TC:Trusted Center) 3 0 0 は、コンテンツ編集エンティティ (AS:Authoring Studio) 3 3 0、および情報記録媒体製造エンティティ (DM:Disc Manufacturer) 3 5 0 に対して様々な管理情報を提供し、コンテンツ編集エンティティ (AS:Authoring Studio) 3 3 0、および情報記録媒体製造エンティティ (DM:Disc Manufacturer) 3 5 0 は、管理センタ (TC:Trusted Center) 3 0 0 から受領した管理情報に基づいて、コンテンツ編集、暗号化、鍵情報の、生成、格納処理などを行う。

#### 【0158】

管理センタ 3 0 0、コンテンツ編集エンティティ 3 3 0、および情報記録媒体製造エンティティ 3 5 0 の実行する処理の詳細について、図 1 7 以下を参照して説明する。

#### 【0159】

図 1 7 には、管理センタ 3 0 0、コンテンツ編集エンティティ 3 3 0、および情報記録媒体製造エンティティ 3 5 0 の実行する処理を示している。

#### 【0160】

管理センタ 3 0 0 は、コンテンツ保持者からのコンテンツ 5 0 1 を保持し、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応してメディアキー Km 5 0 2、第 2 タイトルキー Kt 2, 5 0 3、第 1 タイトルキー Kt 1, 5 0 4、編集スタジオコード (ASC) 5 0 5、情報記録媒体製造者コード (DMC) 5 0 6、ディスク固有シード S 5 0 7、製造を許容する情報記録媒体の数、量産発注枚数 N 5 0 8 を設定する。

#### 【0161】

管理センタ 3 0 0 は、コンテンツ保持者からのコンテンツ 5 0 1 に対して、ステップ S 4 1 において、編集スタジオコード (ASC) 5 0 5、情報記録媒体製造者コード (DMC) 5 0 6 を電子透かしとして埋め込む。

#### 【0162】

ステップ S 4 2 では、ディスク固有シード S 5 0 7 に基づいて、ディスク固有

キーKd511を生成する。

【0163】

管理センタ300は、電子透かしを埋め込んだコンテンツと、編集スタジオコード(ASC)505、情報記録媒体製造者コード(DMC)506、および、ディスク固有シードS507に基づいて生成したディスク固有キーKd511をコンテンツ編集エンティティ330に提供する。

【0164】

さらに、管理センタ300は、ステップS43において、メディアキーKm502をコンテンツ再生権としてのライセンスを持つユーザデバイスのデバイスキーにおいてのみ取得可能な構成とした暗号鍵ブロックとしてのEKB512を生成する。

【0165】

ステップS44では、メディアキーKm502に基づいて第2タイトルキーKt2, 503を暗号化して暗号化第2タイトルキーeKm(Kt2)513を生成し、ステップS45では、メディアキーKm502に基づいて第1タイトルキーKt1, 504を暗号化して暗号化第1タイトルキーeKm(Kt1)514を生成する。

【0166】

さらに、ステップS46において、編集スタジオコード(ASC)505を第2タイトルキーKt2, 503で暗号化し、暗号化ASCであるeKt2(ASC)515を生成し、ステップS47において、情報記録媒体製造者コード(DMC)506を第2タイトルキーKt2, 503で暗号化し、暗号化DMCであるeKt2(DMC)516を生成する。

【0167】

さらに、ディスク固有シードS507に対応して、製造を許容する情報記録媒体の数、量産発注枚数N508に基づくN個の(S, Sig)、すなわちN個の個別ディスクID517を生成する。

【0168】

EKB512、暗号化第2タイトルキーeKm(Kt2)513、暗号化第1

タイトルキー  $eK_m$  ( $K_{t1}$ ) 514、暗号化ASCである  $eK_{t2}$  (ASC) 515、暗号化DMCである  $eK_{t2}$  (DMC) 516、N個の個別ディスクID 517と第1タイトルキー  $K_{t1}$  は、管理センタ300から、情報記録媒体製造エンティティ350に提供される。

#### 【0169】

次に、コンテンツ編集エンティティ330の処理について説明する。コンテンツ編集エンティティ330は、管理センタ300から受領した電子透かし埋め込み済みのコンテンツの符号化、例えばMPEG符号化処理をエンコーダ531において実行し、トランスポートストリームデータを生成し、さらに、管理センタ300から受領した編集スタジオコード(ASC)と、情報記録媒体製造者コード(DMC)の埋め込み処理をPMT(Program Map Table)埋め込み部532において実行する。PMTは編集スタジオコード(ASC)と、情報記録媒体製造者コード(DMC)を含む情報であり、コンテンツ編集エンティティ330においてコンテンツに対して埋め込まれる。

#### 【0170】

PMT(Program Map Table)埋め込み部532において実行する編集スタジオコード(ASC)と、情報記録媒体製造者コード(DMC)を含むPMTの埋め込み処理の詳細について、図18以下を参照して説明する。

#### 【0171】

図18は、ISO/IEC13818-1:1996(MPEGシステム)で規定されているPMT構成、および、本発明において提案する編集スタジオコード(ASC)や情報記録媒体製造者コード(DMC)の格納位置について示す図である。

#### 【0172】

ISO/IEC13818-1:1996(MPEGシステム)では、プログラムマップテーブル(PMT)のデータ構成を図18に示すように規定している。

#### 【0173】

先頭に8ビットのテーブルIDの格納位置が規定され、テーブルIDに続いて

、76ビットの様々な制御情報、識別情報の格納領域が規定されている。その後、プログラム情報領域のデータ長情報であるプログラム情報レングス格納領域が12ビット設定され、その後にプログラム情報レングスに規定されたデータ長を持つプログラム情報領域540が設定される。プログラム情報領域540の後には、コンテンツを構成するビデオデータ、オーディオデータ単位の制御情報としてのエレメンタリストリーム情報が各データ単位に格納され、最後に巡回冗長検査コードとしての32ビットのCRC (Cyclic Redundancy Code) が格納される。

#### 【0174】

ここで、プログラム情報領域540には、任意の追加情報を格納することのできる領域が設定可能であり、ここに編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を格納する。なお、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)は、前述したように、それぞれ、編集スタジオの識別子、情報記録媒体製造者識別子として設定したコードデータとするのみならず、記録媒体の製造単位(ロット)毎、発注単位毎の設定コードとしてもよく、あるいは、記録媒体に格納するコンテンツ毎に設定したコードとしてもよい。さらに、コンテンツ格納記録媒体の発注日時、製造日時等の日時情報などを含めたコードとして設定することも可能である。

#### 【0175】

これらの編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)は、コンテンツ編集エンティティ330が、管理センタ300から受領し、コンテンツ中に埋め込むとともに、暗号処理部533(図17参照)においてシード2を適用して生成するブロックキーKb2に基づく暗号化によって確実に暗号化されて情報記録媒体製造エンティティに渡すことが必要となる。

#### 【0176】

すなわち、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)は、管理センタ300およびコンテンツ編集エンティティ330のみが知り得る情報とし、外部に漏洩され悪用されることを防止する構成とする。

#### 【0177】

従って、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) は、ブロックキー K b 2 に基づく暗号化対象領域に確実に配置されなければならない。基本的にコンテンツ、プログラムマップテーブル (PMT) を格納したソースパケットのほとんどのデータ領域は、シード 2 を用いて生成されるブロックキー K b 2 によって暗号化される領域とされる。しかし、唯一ブロックキー K b 2 の生成情報として利用されるシード 2 の格納領域がブロックキー K b 2 の暗号化領域からはずれることになる。従って、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) のデータ領域が、シード 2 の領域に重ならないように制御することが必要となる。

#### 【0178】

図 19 に示すように、暗号化処理単位として設定される 1 A U (A l l i n e d U n i t) 毎にシード 2 が設定され、各処理単位毎に設定されたシード 2 を利用して暗号化キーとしてのブロックキー K b 2 が生成され、生成されるブロックキー K b 2 によってコンテンツおよびプログラムマップテーブルによって構成される各ソースパケットデータが暗号化されて格納されることになる。

#### 【0179】

従って、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) が暗号処理単位としての 1 A U の先頭部のシード 2 が位置する領域に設定されると、シード 2 として適用される情報となり、その結果、ブロックキー K b 2 での暗号化がなされない平文データのまま、コンテンツ編集エンティティ 330 からディスク製造エンティティに渡されることになる。

#### 【0180】

このような事態の発生を防止するため、コンテンツ編集エンティティ 330 の PMT 埋め込み部 532 では、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) の格納位置を制御した PMT 埋め込みを行うことが必要となる。

#### 【0181】

編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) の格納位置の制御方法としては、2 つの方法がある。

## 【0 1 8 2】

第1の方法は暗号処理単位としての1AU (A l i g n e d U n i t) に含まれる32パケットのうちシード2領域を含むパケットにはプログラムマップテーブル (PMT) を配置しないように制限することである。

## 【0 1 8 3】

PMTパケットの挿入位置を編集時に制御するためには通常のMPEG-TS多重化と異なり、各暗号処理単位 (AU: A l i g n e d U n i t) の先頭 (32パケット単位の先頭) ごとにPMTの配置を禁止するという特殊な多重化処理を必要とする。このようなPMTの配置制御を行うことで、シードD2領域に編集スタジオコード (A S C) と情報記録媒体製造者コード (DMC) が設定されることはなくなる。この場合、PMT内の任意の位置にA S CとDMCを書き込むことができる。

## 【0 1 8 4】

第2の方法はプログラムマップテーブル (PMT) 内において、編集スタジオコード (A S C) と情報記録媒体製造者コード (DMC) の書き込み位置を制御して、PMTパケットが、コンテンツソースパケット中、どの位置に配置された場合でも、編集スタジオコード (A S C) と情報記録媒体製造者コード (DMC) がシード2領域に重ならない構成とする方法である。

## 【0 1 8 5】

この方法について、図20を参照して説明する。図20 (a) は、プログラムマップテーブルPMTの全体データであり、先頭から8ビットがテーブルID、次の76ビットが規定の制御情報、識別情報によって構成され、さらに12ビットのプログラム情報レングスが格納される。その後にプログラム情報が格納される。前述したように追加情報としての編集スタジオコード (A S C) と情報記録媒体製造者コード (DMC) は、このプログラム情報領域中に格納される。

## 【0 1 8 6】

プログラムマップテーブルPMTは、(b) に示すように、先頭のみ183バイトデータ、その後は184バイトデータ毎に区切られて (c) に示すようにTSパケットのペイロードとして格納され、4バイトのヘッダ情報と、先頭パケッ

トについてのみ1バイトのポインタ情報が設定される。さらに(d)に示すようにタイムスタンプ、CCI等のヘッダ情報が付加されたソースパケット(192バイト)とされてコンテンツソースパケット列に点在するように設定される。

#### 【0187】

このとき、シード2として設定される可能性のある部分は、ソースパケットの先頭領域128ビット(16バイト部分)以内の領域である。すなわち、図19に示す暗号処理単位(1AU)の先頭のソースパケットのさらに先頭部分128ビット(16バイト部分)以内の領域がシード2領域として設定される領域であり、この暗号処理単位(1AU)の先頭のソースパケットとして、プログラムマップテーブルPMTの分割データを格納したソースパケットが配置された場合には、そのソースパケットの先頭128ビット部分がシード2として設定される可能性があり、その場合にはこのデータ領域が平文データのまま、コンテンツ編集エンティティ330からディスク製造エンティティに渡されることになる。

#### 【0188】

図20(b)に示すように、先頭パケット(No. 1)は、プログラムマップテーブルPMTの先頭データとして規定される8ビットのテーブルID、76ビットの制御情報、識別情報、さらに12ビットのプログラム情報レングスが必ず格納される。No. 2以下のパケットは、プログラム情報の途中データ以降のデータが格納されることになる。

#### 【0189】

No. 2以下の各パケットには、TSパケットのヘッダ4バイトとソースパケットのヘッダ4バイトの計8バイト=96ビットが先頭に付加されることになるが、もしこの8バイトデータの直後に、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)が存在すると、ソースパケットの先頭128ビット(16バイト)のシード2領域に重なる部分が発生し、平文データのままコンテンツ編集エンティティ330からディスク製造エンティティに渡されることになる。

#### 【0190】

しかし先頭パケット(No. 1)は、プログラムマップテーブルPMTの先頭

データとして規定される 8 ビットのテーブル ID、76 ビットの制御情報、識別情報、さらに 12 ビットのプログラム情報レングスが必ず格納され、その結果、図 20 (e) に示すように、ソースパケットのヘッダ 4 バイト、TS パケットのヘッダ 4 バイト、ポインタ 1 バイト、さらにプログラムマップテーブル PMT の先頭データ 12 バイト (96 ビット) の計 21 バイト (=168 ビット) が設定される。

#### 【0191】

この 21 バイト (=168 ビット) は、シード 2 の最大ビット長 16 バイト (128 ビット) よりも長い。従って、先頭のパケット (No. 1) のペイロードに格納されるプログラム情報領域がシード 2 の設定領域に重なることはない。

#### 【0192】

従って、プログラムマップテーブル PMT 内のプログラム情報領域中において、先頭のパケットに格納されるデータ領域 (PMT の先頭から 183 バイト以内) に編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) を格納する設定とすることで、これらのコードは、必ずブロックキー Kb2 で暗号化される領域となる。

#### 【0193】

すなわち、図 20 (d) に示すように、プログラムマップテーブル PMT の先頭データを格納したソースパケットが、暗号処理単位としての 1 AU の先頭のソースパケットとして設定され、シード 2 領域 541 が設定された場合であっても、そのソースパケットの先頭のシード 2 情報領域として設定される 16 バイト (128 ビット) 領域は、ソースパケットのヘッダ (4 バイト)、TS パケットのヘッダ (4 バイト)、ポインタ (1 バイト)、プログラムマップテーブル PMT の先頭データ 12 バイト (96 ビット) の計 21 バイト (=168 ビット) の領域内に入ることになるため、先頭パケットに含まれるプログラム情報領域はブロックキー Kb2 による暗号化領域 542 として設定され、この領域内に編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) を格納する設定とすることで、これらのコードは、必ずブロックキー Kb2 で暗号化される。

#### 【0194】

このような設定とするためには、をプログラムマッピングテーブルPMT内における編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)の格納位置を制御することが必要となる。すなわち、

①編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)が確実に先頭の packets に含まれる構成とすること。

②先頭の packets の先頭部のシード2領域(128ビット以内)に含まれないこと。

この2つの要件を満足することが必要となる。

#### 【0195】

具体的には、①の条件を満足させるためには、本実施例の場合、先頭のTS packets のペイロード部は183バイトであり、プログラムマッピングテーブルPMTの先頭から183バイト以内に編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を記録することが必要である。

#### 【0196】

また、②の条件を満足させるためには、ソース packets の先頭の128ビット以内に編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)の格納位置を設定されないようにすることである。ただし、これは、図20に示すように、ソース packets のヘッダ4バイトと、TS packets のヘッダおよびポイントの4+1=5バイトと、ISO/IEC13818-1:1996(MPEGシステム)で規定されているPMT構成におけるPMT先頭のキティデータ12バイトの計21バイトが存在し、この領域がシード2領域16バイトよりも大きいので、この後のプログラム情報領域に編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を記録することで、②の条件は満足される。

#### 【0197】

従って、プログラムマッピングテーブルPMTのプログラム情報領域であり、かつ、プログラムマッピングテーブルPMTの先頭から183バイト以内のデータ領域に格納するというPMT内での各コードの格納位置制御を実行することにより、これらのコードがシード2領域に一致することがなくなり、平文データのままコンテンツ編集エンティティ330からディスク製造エンティティに渡されることが

防止される。

#### 【0198】

すわち、図21に示すように、(a)のプログラムマップテーブルPMTの先頭から183バイトまでが、先頭のTSパケットのペイロードとして格納される情報領域であり、この位置に含まれるプログラム情報領域内に編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)の格納位置を設定する。

#### 【0199】

この結果、(b)、(c)に示すように、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)を格納したプログラム情報領域はブロックキーKb2によって暗号化される領域となり、確実にこれらのコードを暗号化してコンテンツ編集エンティティ330からディスク製造エンティティに渡すことが可能となる。

#### 【0200】

コンテンツ編集エンティティ330が、図17に示すPMT(Program Map Table)埋め込み部532において実行する処理をまとめると以下ようになる。すなわち、

(1) 情報記録媒体の製造ルートのエンティティに対応して設定されたエンティティコードである編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)の書き込み位置を制御して制御情報テーブルであるプログラムマップテーブル(PMT)中に設定するエンティティコード設定処理、

(2) 制御情報テーブルを分割格納した複数のパケットを生成するPMT格納パケット生成処理、

(3) PMT格納パケットをコンテンツ格納パケット列に分散配置する処理、である。ここで、(1)のエンティティコード設定処理において、編集スタジオコード(ASC)と情報記録媒体製造者コード(DMC)をシード2の設定領域に重複させることなく、シード2に基づいて生成する鍵(ブロック鍵Kb2)によって暗号化される暗号化領域に含まれるように制御する処理を実行する。

#### 【0201】

なお、本実施例では、識別コードとして編集スタジオコード(ASC)と情報

記録媒体製造者コード（DMC）の適用例について説明したが、前述したように、管理センタの管理するエンティティ、例えばコンテンツ記録媒体の製造、流通過程に存在する様々なエンティティに対応して識別情報（コード）を付与する構成が可能であり、これらの各エンティティに識別コードが付与された場合は、これらの各コードを上記したと同様、ブロックキーK b 2によって確実に暗号化される領域に格納する。

#### 【0 2 0 2】

コンテンツ編集エンティティ 3 3 0 は、上記した処理を、図 1 7 に示す PMT (Program Map Table) 埋め込み部 5 3 2 において実行し、編集スタジオコード（ASC）と、情報記録媒体製造者コード（DMC）を含む PMT の埋め込み処理を行うと、次に、図 1 7 に示す暗号処理部 5 3 3 において暗号処理を実行する。コンテンツ編集エンティティ 3 3 0 の暗号処理部 5 3 3 における処理の詳細について、図 2 2 を参照して説明する。

#### 【0 2 0 3】

コンテンツ編集エンティティ 3 3 0 は、ステップ S 5 1 において乱数に基づいて記録シード（REC SEED）を生成する。記録シード（REC SEED）は出力データとして、情報記録媒体製造エンティティに渡されるデータである。さらに、ステップ S 5 2 において、管理センタ 3 0 0 から受領したディスク固有キーK d と、記録シード（REC SEED）を適用した暗号処理により、記録キーK 2 を生成し、ステップ S 5 3 において、コンテンツ中から選択したシード情報（シード 2）と記録キーK 2 とに基づいてブロックキーK b 2 を生成（ステップ S 5 4）し、ステップ S 5 5 において、ブロックキーK b 2 に基づいて、コンテンツおよびプログラムマップテーブルを含むデータ領域の暗号化処理を実行する。セレクトステップ S 5 3 ではシード 2 を選択するとともに、ステップ S 5 5 における暗号処理を実行するデータ部と、ステップ S 5 5 における暗号処理を実行しないデータ部が分離され、ステップ S 5 6 において暗号処理データと非暗号処理データとが再度結合されて出力データとして、記録シード（REC SEED）とともにディスクイメージデータとして情報記録媒体製造エンティティに渡される。

## 【0204】

コンテンツ編集エンティティ 330 の出力するデータは、図 22 (b) に示すように、シード情報 (シード 2) が平文データとして設定され、その他がシード 2 を適用して生成されるブロック鍵  $K_b 2$  によって暗号化され、この暗号化データ中には、編集スタジオコード (ASC) と、情報記録媒体製造者コード (DMC) とを含む PMT (Program Map Table) が格納されている。

## 【0205】

次に、図 17 に戻り、情報記録媒体製造エンティティ 350 の処理について説明する。情報記録媒体製造エンティティ 350 は、コンテンツ編集エンティティ 350 からの受領コンテンツに対して、まず、暗号処理部 551 において暗号処理を実行する。

## 【0206】

情報記録媒体製造エンティティ 350 の暗号処理部 551 において実行する暗号処理の詳細について図 23 を参照して説明する。

## 【0207】

情報記録媒体製造エンティティ 350 は、ステップ S61 において乱数に基づいて物理インデックスを生成する。さらに、ステップ S62 において、管理センタ 300 から受領した第 1 タイトルキー  $K_t 1$  と、物理インデックスを適用した暗号処理により、記録キー  $K_1$  を生成し、ステップ S63 において、コンテンツ中から選択したシード情報 (シード 1) と記録キー  $K_1$  とに基づいてブロックキー  $K_b 1$  を生成 (ステップ S64) し、ステップ S65 において、ブロックキー  $K_b 1$  に基づいて、コンテンツ中のシード情報 (シード 2) を含むデータ領域の暗号化処理を実行する。セレクトステップ S63 ではシード 1 を選択するとともに、ステップ S65 における暗号処理を実行するデータ部と、ステップ S65 における暗号処理を実行しないデータ部が分離され、ステップ S66 において暗号処理データと非暗号処理データとが再度結合されて出力データとされる。

## 【0208】

情報記録媒体製造エンティティ 350 の暗号処理部 551 の出力するデータは、図 23 (b) に示すように、シード情報 (シード 1) が平文データとして制御

データ (UCD: User control Data) 中に設定され、シード 2 を含むデータ領域がシード 1 を適用して生成されるブロック鍵  $K_b 1$  によって暗号化されたデータとなる。

#### 【0209】

図 17 に戻り、情報記録媒体製造エンティティ 350 の処理について説明を続ける。情報記録媒体製造エンティティ 350 の暗号処理部 551 の出力データは、フォーマット処理部 552 に入力され、管理センタ 300 から受領する  $EKB 512$ 、暗号化第 2 タイトルキー  $eKm (Kt 2) 513$ 、暗号化第 1 タイトルキー  $eKm (Kt 1) 514$ 、暗号化 ASC である  $eKt 2 (ASC) 515$ 、暗号化 DMC である  $eKt 2 (DMC) 516$  をディスクのリードイン領域 (図 1 参照) に書き込む処理を実行する。その書き込み処理の際に、図 23 (a) ステップ S61 において生成された物理インデックスが同時に情報記録媒体に記録される。

#### 【0210】

さらに、これらの情報を有する情報記録媒体 (ディスク) のレプリカを複製製造部 553 において製造する。製造数は、管理センタ 300 の設定した量産発注枚数  $N$  に対応する数であり、各情報記録媒体毎に管理センタ 300 から受領した異なるディスク ID が格納される。

#### 【0211】

これらの全情報の格納処理がなされると、情報記録媒体 100 が市場に流通し、ユーザに提供されユーザの情報処理装置において、前述した復号処理および再生制御処理に基づいてコンテンツ再生が実行される。情報記録媒体 100 は、図 1 を参照して説明した各種の情報を格納し、ユーザの情報処理装置において、図 9 ~ 図 15 を参照して説明した復号、制御に基づく再生が実行される。

#### 【0212】

[ディスク ID を用いない処理構成]

上述した実施例では、情報記録媒体に各媒体毎に異なるディスク ID を設定し、ユーザデバイス側でディスク ID を情報記録媒体から取得し、検証の後、ディスク ID の構成要素としてのディスク固有シード  $S$  を適用してディスク固有キー

Kdを生成(図10ステップS15)し、ディスク固有キーKdを適用したコンテンツ復号を実行する構成を説明した。

#### 【0213】

しかし、情報記録媒体毎に異なるIDを記録する処理は手間がかかる処理であり、大量のディスクを量産する場合には、省略したい場合もある。以下、情報記録媒体毎に異なるディスクIDを用いない処理例について説明する。

#### 【0214】

図24に、管理センタ300、コンテンツ編集エンティティ330、および情報記録媒体製造エンティティ350の実行するディスクIDを用いない処理例を示している。

#### 【0215】

図24において点線枠領域600の構成が、先に図17を参照して説明したディスクIDを適用した処理例と異なる部分である。なお、先に図17を参照して説明したディスクID関連の処理、構成は、図24には示されていない。

#### 【0216】

管理センタ300は、コンテンツ保持者からのコンテンツ501を保持し、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応してメディアキーKm502、第2タイトルキーKt2, 503、第1タイトルキーKt1, 504、編集スタジオコード(ASC)505、情報記録媒体製造者コード(DMC)506、さらに、製造するメディアとしての情報記録媒体に格納するコンテンツあるいはメディアに対応して設定される第3タイトルキーKt3, 601を設定する。

#### 【0217】

本例においては、図17を参照して説明したディスク固有シードS507、製造を許容する情報記録媒体の数、すなわち量産発注枚数N508が省略される。

#### 【0218】

管理センタ300は、コンテンツ保持者からのコンテンツ501に対して、ステップS41において、編集スタジオコード(ASC)505、情報記録媒体製造者コード(DMC)506を電子透かしとして埋め込む。

## 【0 2 1 9】

管理センタ 3 0 0 は、電子透かしを埋め込んだコンテンツと、編集スタジオコード (A S C) 5 0 5、情報記録媒体製造者コード (D M C) 5 0 6、および、ディスク固有キー (Disc Unique Key)  $K_d$ , 5 1 1 をコンテンツ編集エンティティ 3 3 0 に提供する。

## 【0 2 2 0】

さらに、管理センタ 3 0 0 は、ステップ S 4 3 において、メディアキー  $K_m$  5 0 2 をコンテンツ再生権としてのライセンスを持つユーザデバイスのデバイスキーにおいてのみ取得可能な構成とした暗号鍵ブロックとしての  $E K B$  5 1 2 を生成する。

## 【0 2 2 1】

ステップ S 4 4 では、メディアキー  $K_m$  5 0 2 に基づいて第 2 タイトルキー  $K_t$  2, 5 0 3 を暗号化して暗号化第 2 タイトルキー  $e K_m (K_t 2)$  5 1 3 を生成し、ステップ S 4 5 では、メディアキー  $K_m$  5 0 2 に基づいて第 1 タイトルキー  $K_t$  1, 5 0 4 を暗号化して暗号化第 1 タイトルキー  $e K_m (K_t 1)$  5 1 4 を生成する。

## 【0 2 2 2】

さらに、ステップ S 4 6 において、編集スタジオコード (A S C) 5 0 5 を第 2 タイトルキー  $K_t$  2, 5 0 3 で暗号化し、暗号化 A S C である  $e K_t 2 (A S C)$  5 1 5 を生成し、ステップ S 4 7 において、情報記録媒体製造者コード (D M C) 5 0 6 を第 2 タイトルキー  $K_t$  2, 5 0 3 で暗号化し、暗号化 D M C である  $e K_t 2 (D M C)$  5 1 6 を生成する。

## 【0 2 2 3】

さらに、ステップ S 7 1 において、第 3 タイトルキー  $K_t$  3, 6 0 1 をメディアキー  $K_m$  5 0 2 に基づいて暗号化して暗号化第 3 タイトルキー  $e K_m (K_t 3)$  6 0 2 を生成する。

## 【0 2 2 4】

$E K B$  5 1 2、暗号化第 2 タイトルキー  $e K_m (K_t 2)$  5 1 3、暗号化第 1 タイトルキー  $e K_m (K_t 1)$  5 1 4、暗号化 A S C である  $e K_t 2 (A S C)$

515、暗号化DMCである  $eKt2$  (DMC) 516、暗号化第3タイトルキー  $eKm(Kt3)$  602は、管理センタ300から、情報記録媒体製造エンティティ350に提供される。

#### 【0225】

コンテンツ編集エンティティ330の処理、情報記録媒体製造エンティティ350の処理は、基本的に先に図17～図23を参照して説明した処理と同様である。ただし、情報記録媒体製造エンティティ350のフォーマット処理部552は、情報記録媒体のリードイン領域に書き込む処理を実行し、情報記録媒体製造エンティティ350の複製製造部553は、ディスク毎のディスクIDの書き込み処理を実行しない。

#### 【0226】

この結果として製造される情報記録媒体100は、図25に示すようなデータを格納することになる。

#### 【0227】

図25に示すように、情報記録媒体100には、物理インデックス102、暗号化コンテンツ103、記録シード (REC SEED) 104、暗号鍵情報120が格納される。暗号鍵情報120は、情報記録媒体100のコンテンツ格納領域とは異なる特別のプログラムに基づいて読み取り可能なリードイン領域110に格納される。

#### 【0228】

暗号鍵情報120には、暗号化第3タイトルキー  $eKm(Kt3)$  が含まれる。図1の構成と異なる点は、ディスクIDが格納されない点と、暗号鍵情報120に暗号化第3タイトルキー  $eKm(Kt3)$  611が追加された点である。

#### 【0229】

この情報記録媒体を再生する情報処理装置 (ユーザデバイス) の暗号処理手段の実行するコンテンツ復号処理について図26を参照して説明する。

#### 【0230】

図26の処理中、先に図10を参照して説明したディスクIDを持つ情報記録媒体の再生処理と異なる点は、情報記録媒体100が、暗号化第3タイトルキー

e Km (K t 3) 6 1 1 を持つ点、ステップ S 8 2 のディスク固有キー K d の生成処理、ステップ S 8 1 の暗号化第 3 タイトルキー e Km (K t 3) 6 1 1 の復号処理である。

#### 【0231】

本実施例においては、ディスク固有キー K d の生成処理をディスク ID から取得したディスク固有シード S (図 10, ステップ S 14 参照) を適用しない。

#### 【0232】

本実施例では、ステップ S 8 1 において、暗号化第 3 タイトルキー e Km (K t 3) 6 1 1 をメディアキー Km を用いて復号して、第 3 タイトルキー K t 3 を取得し、取得した第 3 タイトルキー K t 3 と、ステップ S 12 の復号処理で取得した第 2 タイトルキー K t 2 に基づく暗号処理をステップ S 8 2 において実行してディスク固有キー K d の生成処理を実行する構成としている。

#### 【0233】

以下の処理は、先に図 10 を参照して説明した処理と同様である。本処理例においては、ディスク ID を用いない構成であるので、情報記録媒体毎に異なる ID を記録する処理が不要となり、大量のディスクを量産する場合等、情報記録媒体製造エンティティの処理が軽減される。

#### 【0234】

本例においても、情報記録媒体に格納されたコンテンツは、シード情報 (シード 1) およびシード情報 (シード 2) によって生成されるブロック鍵 K b 1, K b 2 で暗号化され、シード情報 (シード 2) は、シード情報 (シード 1) を用いて生成される鍵、すなわちブロックキー K b 1 によって暗号化されて格納されるので、情報記録媒体からの直接読み取りが不可能となり、シード情報 (シード 2) の解析、シード情報 (シード 2) を適用して生成するブロックキー K b 2 の解析、ブロックキー K b 2 によって暗号化されるユーザデータの暗号化アルゴリズムの解析困難性を高めることが可能となる。

#### 【0235】

さらに、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) は、シード情報 (シード 2) を適用して生成するブロックキー K b 2 によって

確実に暗号化される領域に設定され、コンテンツ編集エンティティ 330 において暗号化された後、情報記録媒体製造エンティティ 350 に渡されることになり、これらのコード情報の外部漏洩が防止される。

#### 【0236】

さらに、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) の検出、照合一致を条件として再生処理を実行する構成としたので、不正なコードあるいは電子透かしを持たないコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となり、また不正な複製が製造され、流通した場合において、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

#### 【0237】

##### [情報処理装置他のエンティティ構成例]

次に、上述した各実施例において説明したユーザデバイスとしての情報処理装置、管理センタ、コンテンツ編集エンティティ、情報記録媒体製造エンティティ、各エンティティが暗号処理、データ生成処理を実行するために適用する情報処理装置の構成例を図 27 を参照して説明する。上述した各実施例において説明したユーザデバイスとしての情報処理装置、管理センタ、コンテンツ編集エンティティ、情報記録媒体製造エンティティ、各エンティティが暗号処理、データ生成処理を実行するために適用する情報処理装置としては、例えば PC、情報処理サーバ等の汎用的な情報処理装置が適用可能である。以下、図 27 を参照して、上述した各エンティティが暗号処理、データ生成処理を実行するために適用する情報処理装置の構成例について説明する。

#### 【0238】

CPU (Central Processing Unit) 701 は、ROM (Read Only Memory) 702 に記憶されている各種プログラム、あるいは、記憶部 708 に格納され、RAM (Random Access Memory) 703 にロードされたプログラムに従って各種処理を実行する。タイマ 700 は計時処理を行ない、クロック情報を CPU 701 に供給する。

## 【0239】

ROM (Read Only Memory) 702は、CPU 701が使用するプログラムや演算用のパラメータ、固定データ等を格納する。RAM (Random Access Memory) 703は、CPU 701の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を格納する。これら各素子はバス711により相互に接続されている。

## 【0240】

暗号処理部704は、上述した各種の暗号処理、例えばAES暗号化アルゴリズムを適用した暗号処理等を実行する。WM処理部713は、例えばスペクトラム拡散技術を用いて、データを不可視な情報としてビデオ信号へ埋め込む、あるいはデータを認識できない情報としてオーディオ信号へ埋め込む、などインフォメーションハイディング (Information Hiding) 技術に基づく処理を実行する。

## 【0241】

入出力インタフェース712には、キーボード、マウス等の入力部706、CRT、LCD等のディスプレイ、スピーカ等からなる出力部707、ハードディスク等の記憶部708、通信部709が接続される。通信部709は、例えばインターネット等の通信網を介したデータ送受信により、たとえば各エンティティ間の通信を行なう。

## 【0242】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

## 【0243】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用

のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

#### 【0244】

例えば、プログラムは記録媒体としてのハードディスクやROM (Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、CD-ROM (Compact Disc Read Only Memory)、MO (Magneto optical)ディスク、DVD (Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウェアとして提供することができる。

#### 【0245】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、LAN (Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記録媒体にインストールすることができる。

#### 【0246】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。また、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

#### 【0247】

##### 【発明の効果】

以上、説明したように、本発明の構成によれば、編集スタジオコード (ASC) と情報記録媒体製造者コード (DMC) 等のエンティティコードを情報記録媒体に確実に暗号化して格納することが可能となり、外部に対するこれらのエンティティコードの漏洩が防止される。従って、不正にこれらのエンティティコード

を取得して、正規のエンティティになりすました不正コピーコンテンツ格納媒体の製造を防止できる。すなわち、各コードが鍵生成情報としてのシード領域に重ならないようにプログラムマップテーブル（PMT）内でのデータ設定位置を制御する構成としたので、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を格納したプログラムマップテーブルの格納パッケージをコンテンツパッケージ列の任意の位置に設定した場合でも、各エンティティコードが非暗号化データとしてのシード領域に重なることがなく、コードの外部漏洩を防止できる。

#### 【0248】

さらに、本発明の構成では、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を情報記録媒体に暗号化コンテンツとともに格納し、これらのコードが正しく検出され、照合されたことを条件として再生処理を実行する構成としたので、不正なコードの格納された媒体や、コードを格納していない情報記録媒体に格納されたコンテンツの再生は停止され、正当な製造ルートに基づいて製造されたコンテンツ格納記録媒体のみが再生可能となる。また不正な情報記録媒体の複製が製造され、流通した場合において、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を検出することにより、情報の漏洩ルートを容易に追跡することが可能となる。

#### 【0249】

さらに、本発明の構成によれば、各エンティティのコード情報を情報記録媒体に格納する構成としたので、管理センタによって管理されたコンテンツ編集エンティティおよび情報記録媒体製造エンティティのみが正規な暗号化コンテンツを編集し、情報記録媒体を製造することが可能となり、情報記録媒体が不正に複製された場合には、コード検出による情報漏洩ルートの解析が可能となる。

#### 【図面の簡単な説明】

##### 【図1】

情報記録媒体に格納されるデータ構成について説明する図である。

##### 【図2】

情報記録媒体に格納されるデータの管理、情報記録媒体の製造ルートについて

説明する図である。

【図 3】

各種キー、データの暗号化処理、配布処理に適用される階層型木構造を説明する図である。

【図 4】

各種キー、データの配布に使用される有効化キーブロック（E K B）の例を示す図である。

【図 5】

コンテンツ鍵の有効化キーブロック（E K B）を使用した配布例と復号処理例を示す図である。

【図 6】

情報記録媒体に格納されるデータ構成について説明する図である。

【図 7】

情報記録媒体に格納される編集スタジオコード（A S C）と情報記録媒体製造者コード（D M C）を含むプログラムマップテーブル P M T について説明する図である。

【図 8】

情報処理装置の構成例について説明する図である。

【図 9】

情報処理装置において実行するコンテンツ復号、再生制御処理について説明する図である。

【図 1 0】

情報処理装置において実行するコンテンツ復号処理について説明する図である。

【図 1 1】

ディスク固有キーの生成処理例について説明する図である。

【図 1 2】

暗号化データの復号処理シーケンスを説明する図である。

【図 1 3】

コンテンツの再生制御処理について説明する図である。

【図 1 4】

コンテンツの復号処理および再生制御処理の手順について説明するフローチャートを示す図である。

【図 1 5】

コンテンツの復号処理および再生制御処理の手順について説明するフローチャートを示す図である。

【図 1 6】

シード情報の格納構成例について説明する図である。

【図 1 7】

各エンティティ毎の情報記録媒体に対して実行するデータ格納、暗号化処理を説明する図である。

【図 1 8】

編集スタジオコード (A S C) と情報記録媒体製造者コード (D M C) を含むプログラムマップテーブル P M T データ構成について説明する図である。

【図 1 9】

暗号処理単位としての 1 A U ごとのシード 2 の設定構成を説明する図である。

【図 2 0】

編集スタジオコード (A S C) と情報記録媒体製造者コード (D M C) の格納位置について説明する図である。

【図 2 1】

編集スタジオコード (A S C) と情報記録媒体製造者コード (D M C) の格納位置について説明する図である。

【図 2 2】

コンテンツ編集エンティティの実行する暗号処理を説明する図である。

【図 2 3】

情報記録媒体製造エンティティの実行する暗号処理を説明する図である。

【図 2 4】

ディスク I D を用いない処理例における各エンティティ毎の情報記録媒体に対

して実行するデータ格納、暗号化処理を説明する図である。

【図 2 5】

ディスク I D を用いない処理例における情報記録媒体に格納されるデータ構成について説明する図である。

【図 2 6】

ディスク I D を用いない処理例における情報処理装置において実行するコンテンツ復号処理について説明する図である。

【図 2 7】

ユーザデバイス、各エンティティにおいて適用する情報処理装置の構成例を示す図である。

【符号の説明】

- 1 0 0 情報記録媒体
- 1 0 1 ディスク I D
- 1 0 2 物理インデックス
- 1 0 3 暗号化コンテンツ
- 1 0 4 記録シード
- 1 1 0 リードイン領域
- 1 2 0 暗号鍵情報
- 1 2 1 E K B
- 1 2 2 暗号化第 1 タイトルキー  $e K m (K t 1)$
- 1 2 3 暗号化第 2 タイトルキー  $e K m (K t 2)$
- 1 2 4 暗号化 A S C,  $e K t 2 (A S C)$
- 1 2 5 暗号化 D M C :  $e K t 2 (D M C)$
- 2 0 0 情報処理装置
- 3 0 0 管理センタ
- 3 3 0 コンテンツ編集エンティティ
- 3 5 0 情報記録媒体製造エンティティ
- 2 1 0 バス
- 2 2 0 入出力インタフェース

- 2 3 0 M P E G コーデック
- 2 4 0 入出力インタフェース
- 2 4 1 A / D , D / A コンバータ
- 2 5 0 暗号処理手段
- 2 5 5 再生制御処理手段
- 2 6 0 R O M
- 2 7 0 C P U
- 2 8 0 メモリ
- 2 9 0 記録媒体 I / F
- 2 9 5 記録媒体
- 2 9 8 T S 処理手段
- 4 0 1 E K B
- 4 0 2 暗号化第 2 タイトルキー e K m ( K t 2 )
- 4 0 3 暗号化第 1 タイトルキー e K m ( K t 1 )
- 4 0 4 ディスク I D
- 4 0 5 記録シード
- 4 0 6 物理インデックス
- 4 0 7 暗号化コンテンツ
- 4 1 0 デバイスキー
- 4 1 1 第 2 タイトルキー K t 2
- 4 1 2 コンテンツ
- 4 2 0 暗号処理単位
- 4 2 1 制御データ
- 4 2 2 先頭 T S パケット
- 4 2 3 後続 T S パケット
- 4 2 4 復号 T S パケット
- 4 2 5 復号 T S パケット群
- 4 2 6 復号 T S パケット
- 4 3 1 シード情報 ( シード 1 )

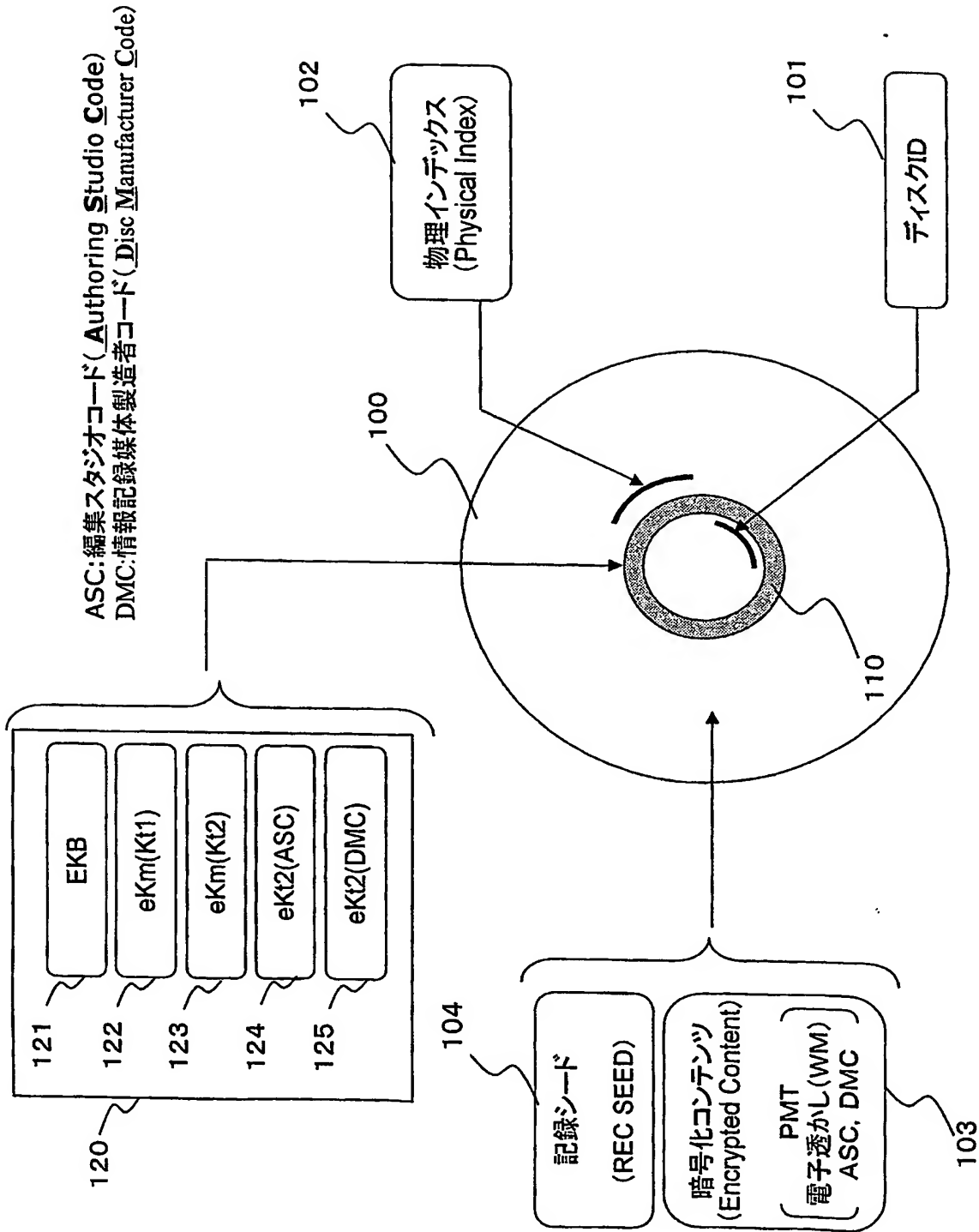
- 4 3 2 シード情報 (シード 2)
- 5 0 1 コンテンツ
- 5 0 2 メディアキー
- 5 0 3 第 1 タイトルキー
- 5 0 4 第 2 タイトルキー
- 5 0 5 コンテンツ編集スタジオコード (A S C : Authoring Studio Code)
- 5 0 6 情報記録媒体製造者コード (D M C : Disc Manufacturer Code)
- 5 0 7 ディスク固有シード S
- 5 0 8 量産発注枚数 N
- 5 1 1 ディスク固有キー K d
- 5 1 2 E K B
- 5 1 3 暗号化第 2 タイトルキー e K m (K t 2)
- 5 1 4 暗号化第 1 タイトルキー e K m (K t 1)
- 5 1 5 暗号化 A S C , e K t 2 (A S C)
- 5 1 6 暗号化 D M C : e K t 2 (D M C)
- 5 1 7 個別ディスク I D
- 5 3 1 エンコーダ
- 5 3 2 P M T 埋め込み部
- 5 3 3 暗号処理部
- 5 4 0 プログラム情報領域
- 5 4 1 シード 2 領域
- 5 4 2 ブロックキー K b 2 による暗号化領域
- 5 5 1 暗号処理部
- 5 5 2 フォーマット処理部
- 5 5 3 複製製造部
- 6 0 1 第 3 タイトルキー K t 3
- 6 0 2 暗号化第 3 タイトルキー e K m (K t 1)
- 6 1 1 暗号化第 3 タイトルキー e K m (K t 1)
- 7 0 0 タイマ

- 7 0 1    C P U (Central processing Unit)
- 7 0 2    R O M (Read-Only-Memory)
- 7 0 3    R A M (Random Access Memory)
- 7 0 4    暗号処理部
- 7 0 6    入力部
- 7 0 7    出力部
- 7 0 8    記憶部
- 7 0 9    通信部
- 7 1 0    ドライブ
- 7 1 1    バス
- 7 1 2    入出力インタフェース
- 7 1 3    WM(Watermark)処理部
- 7 2 1    リムーバブル記録媒体

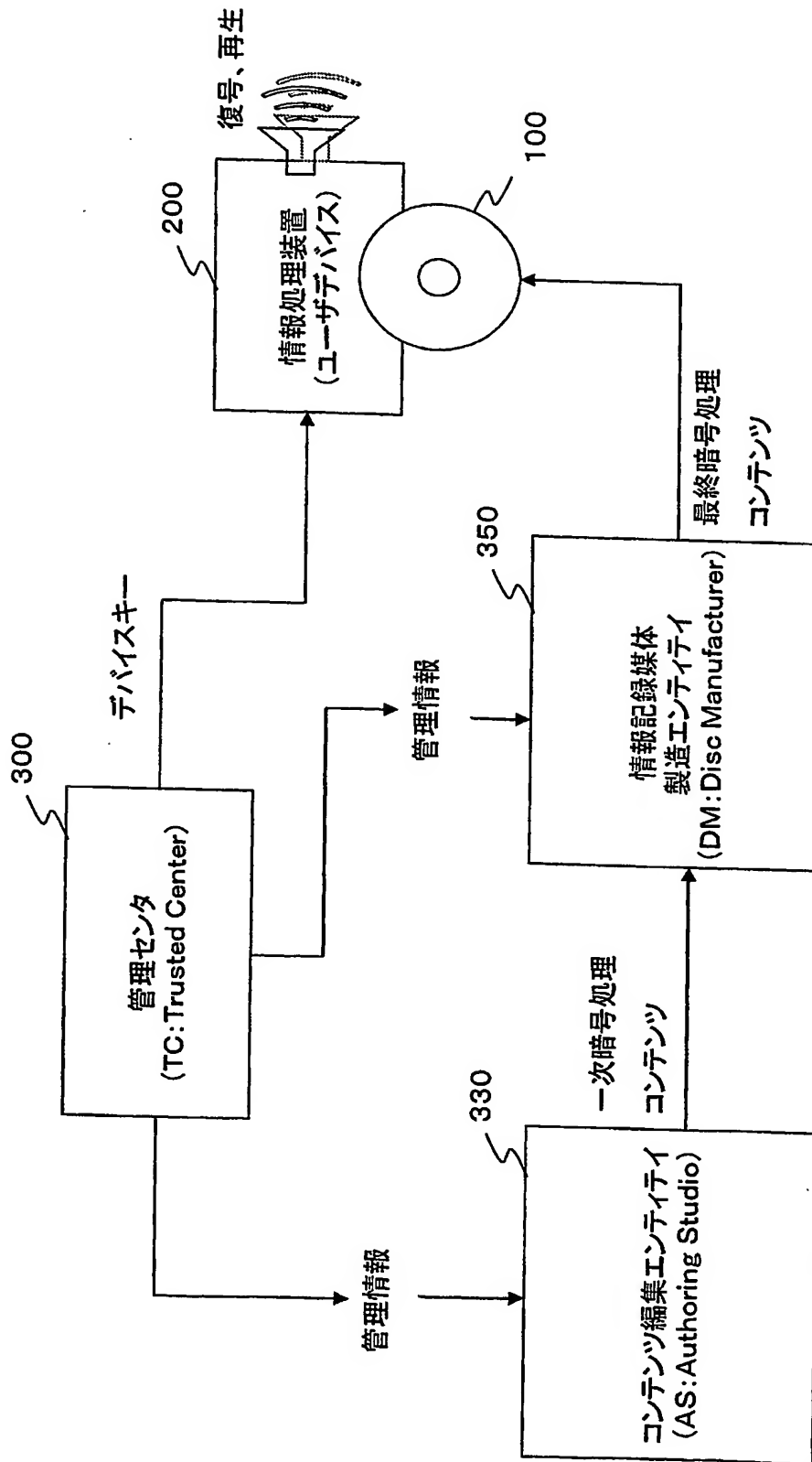
【書類名】

図面

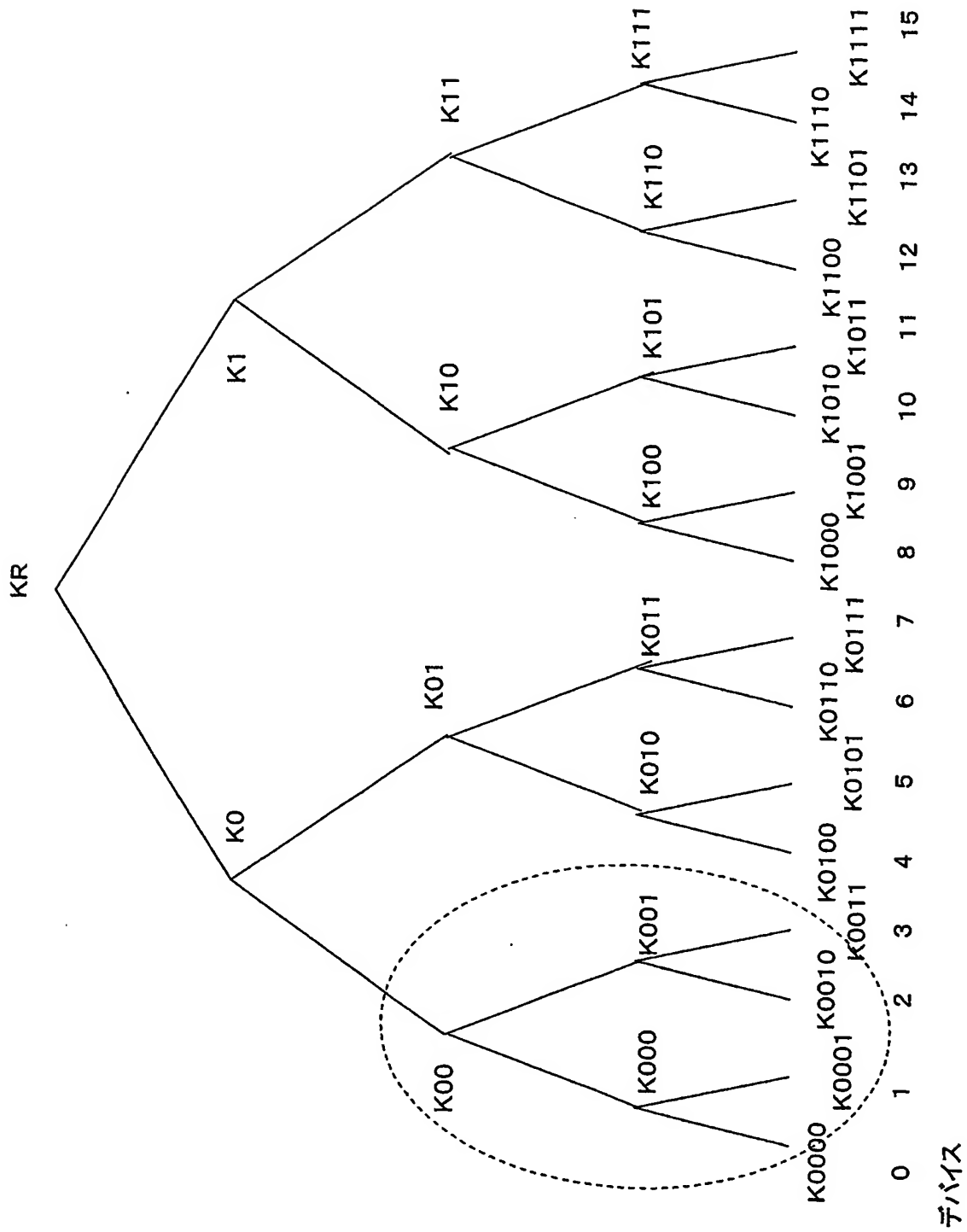
【図 1】



【図 2】



【図 3】



【図 4】

(A) 有効化キーブロック  
(EKB:Enabling Key Block)例1

(B) 有効化キーブロック  
(EKB:Enabling Key Block) 例2

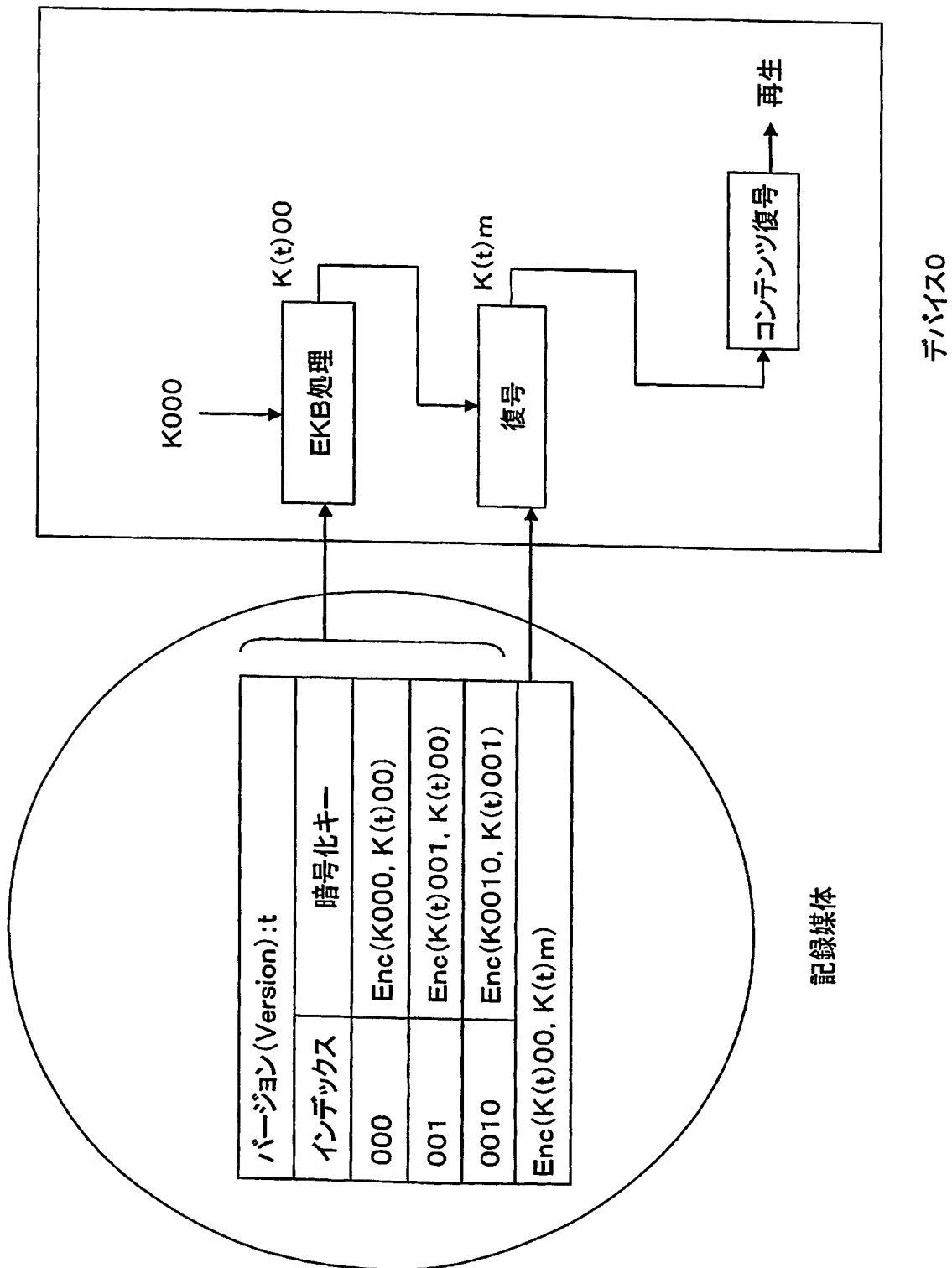
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	$\text{Enc}(K(t)0, K(t)R)$
00	$\text{Enc}(K(t)00, K(t)0)$
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

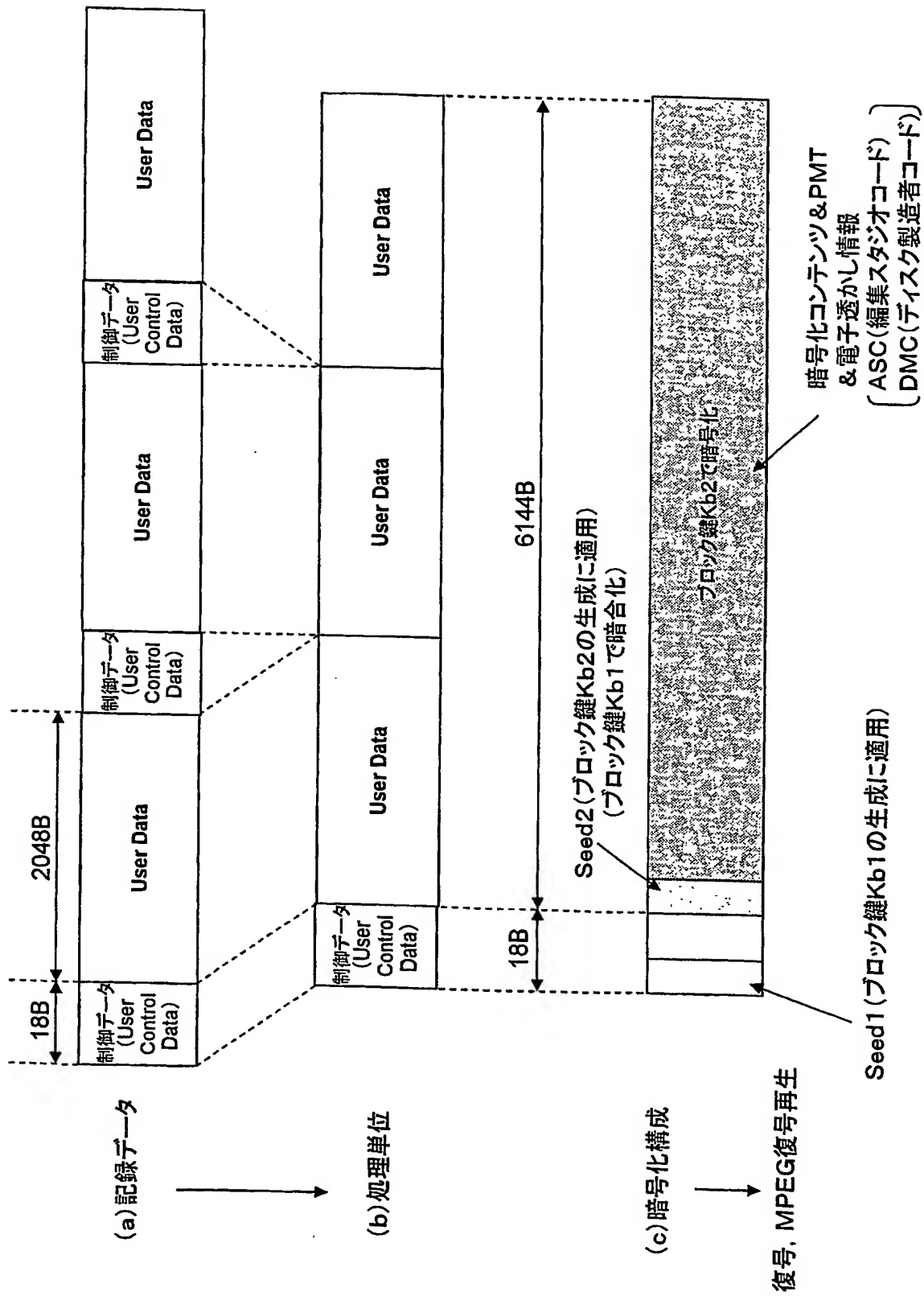
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	$\text{Enc}(K000, K(t)00)$
001	$\text{Enc}(K(t)001, K(t)00)$
0010	$\text{Enc}(K0010, K(t)001)$

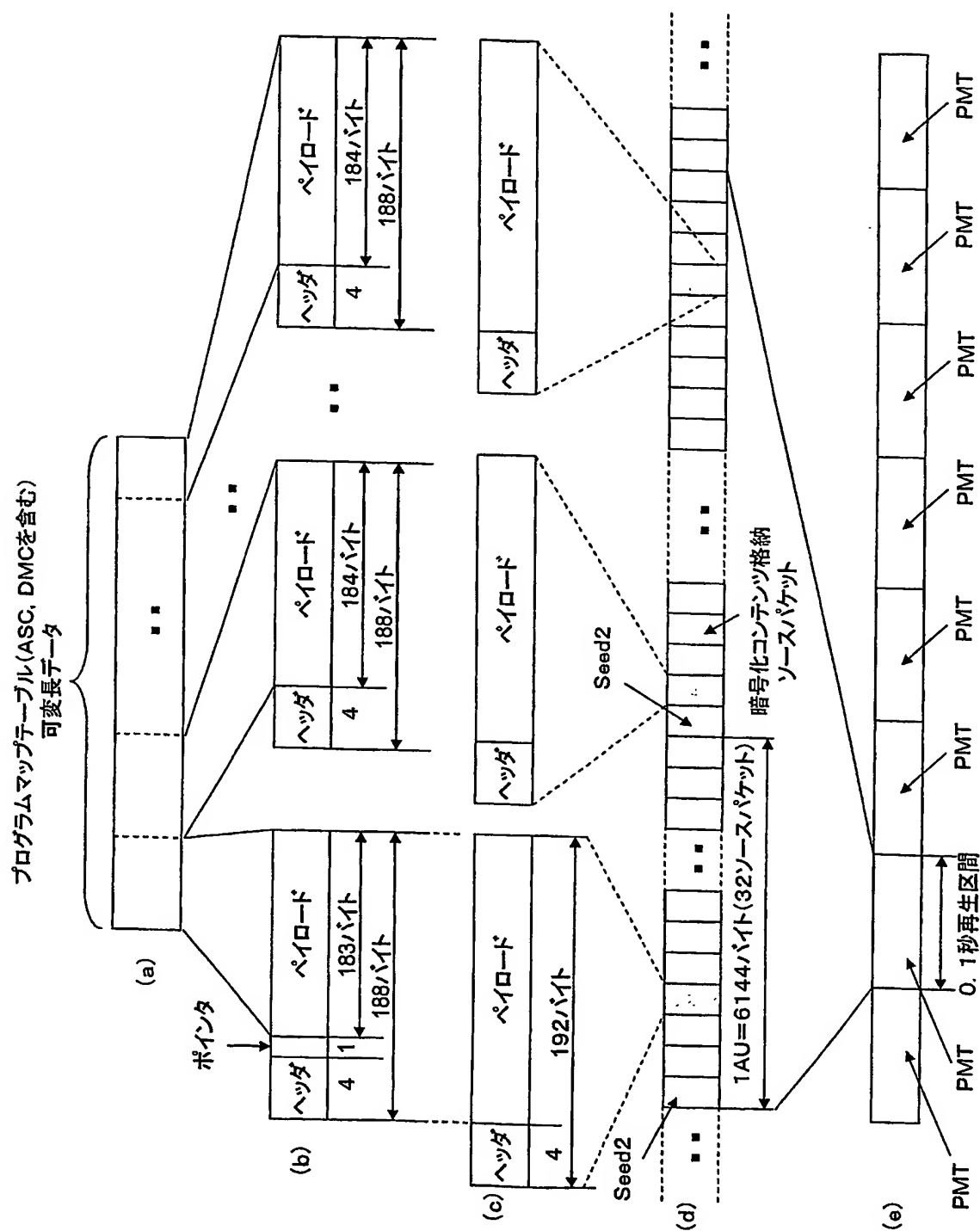
【図 5】



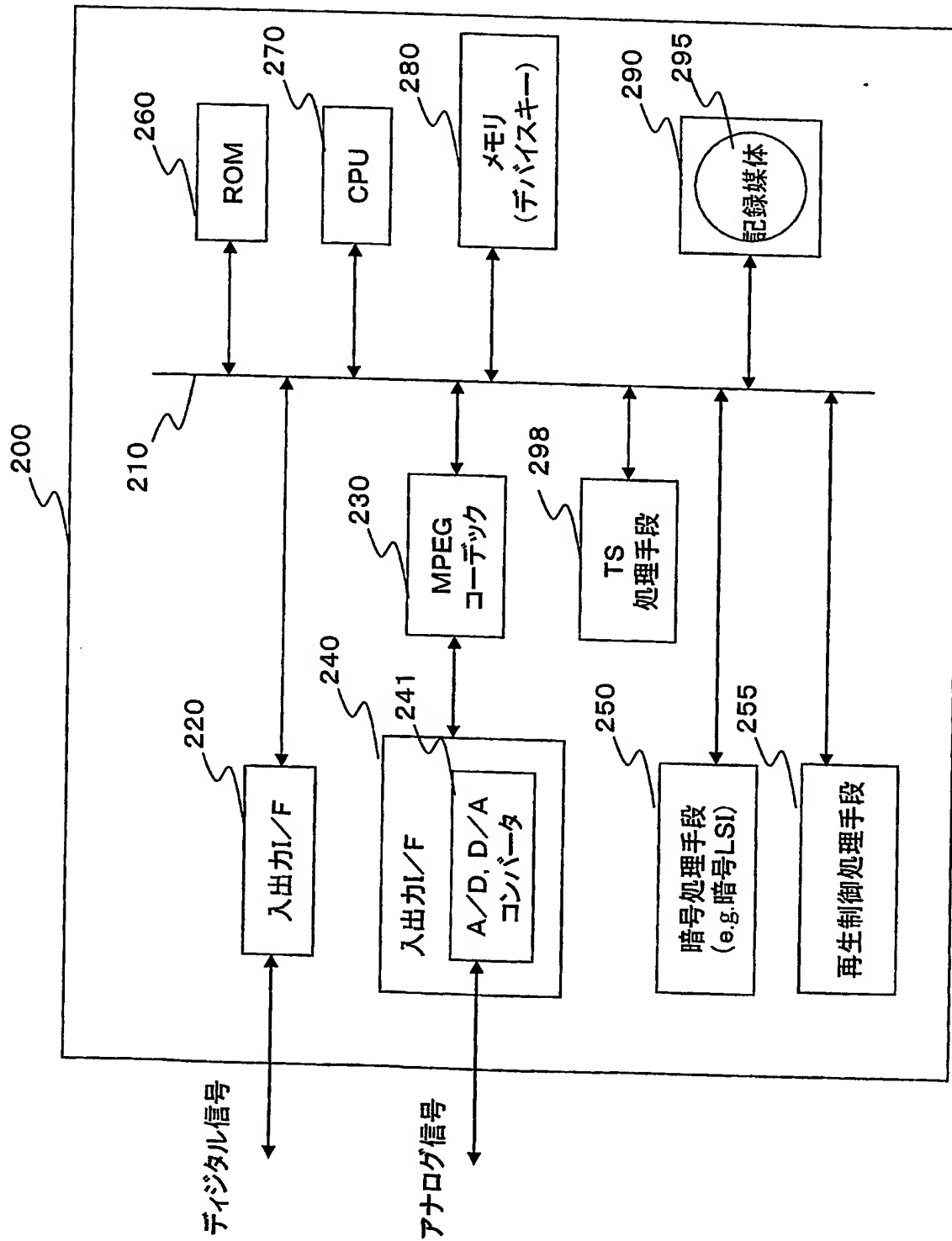
【図 6】



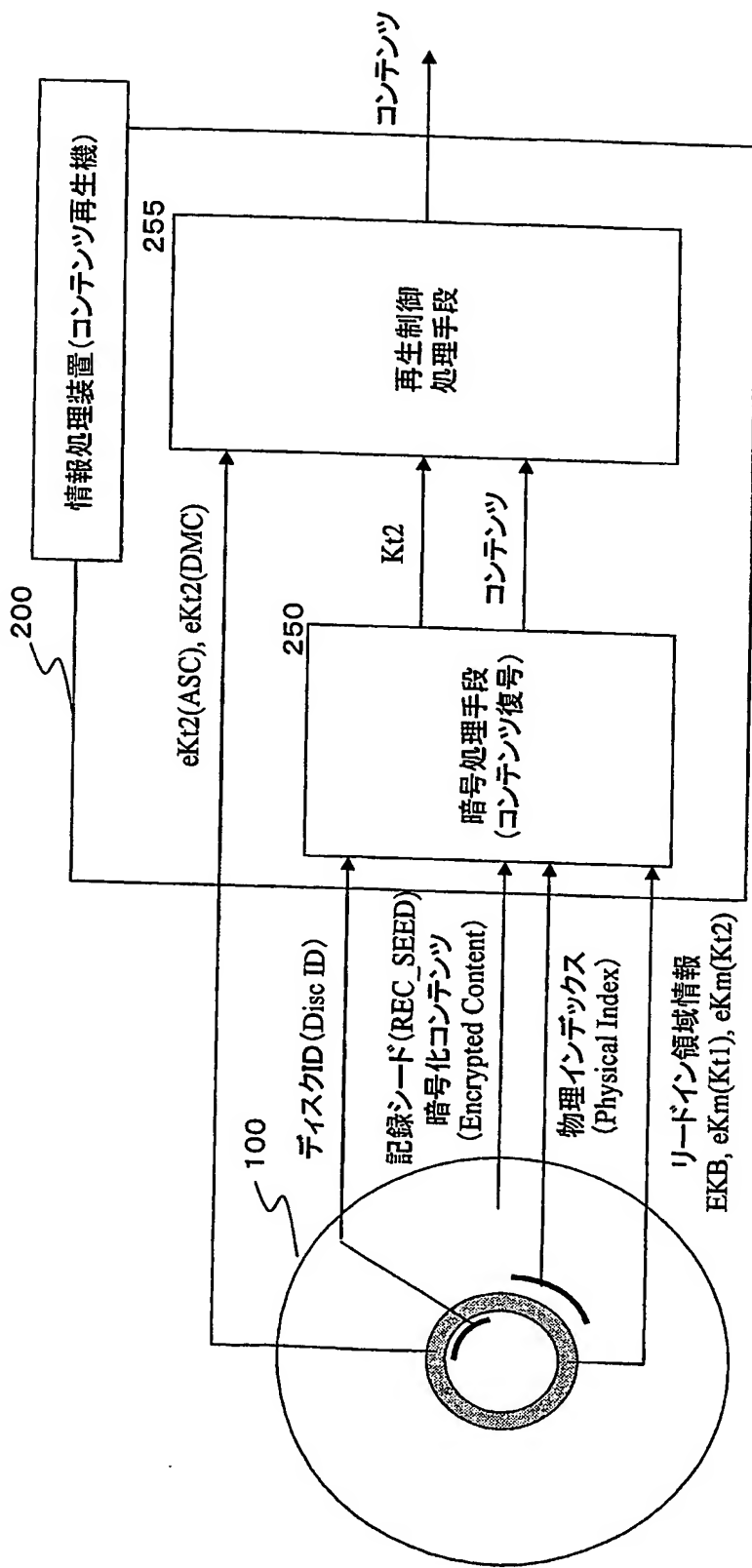
【図 7】



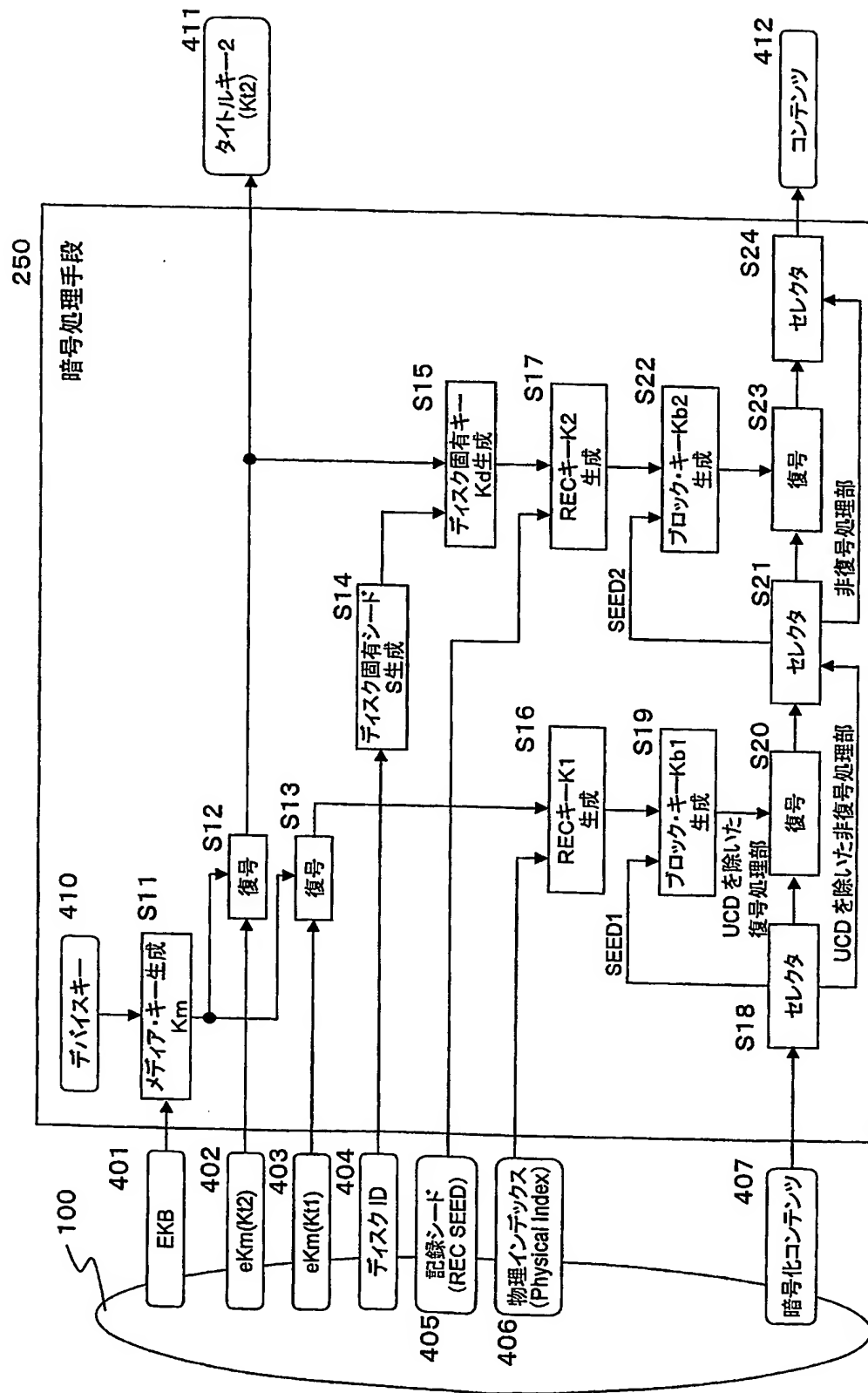
【図 8】



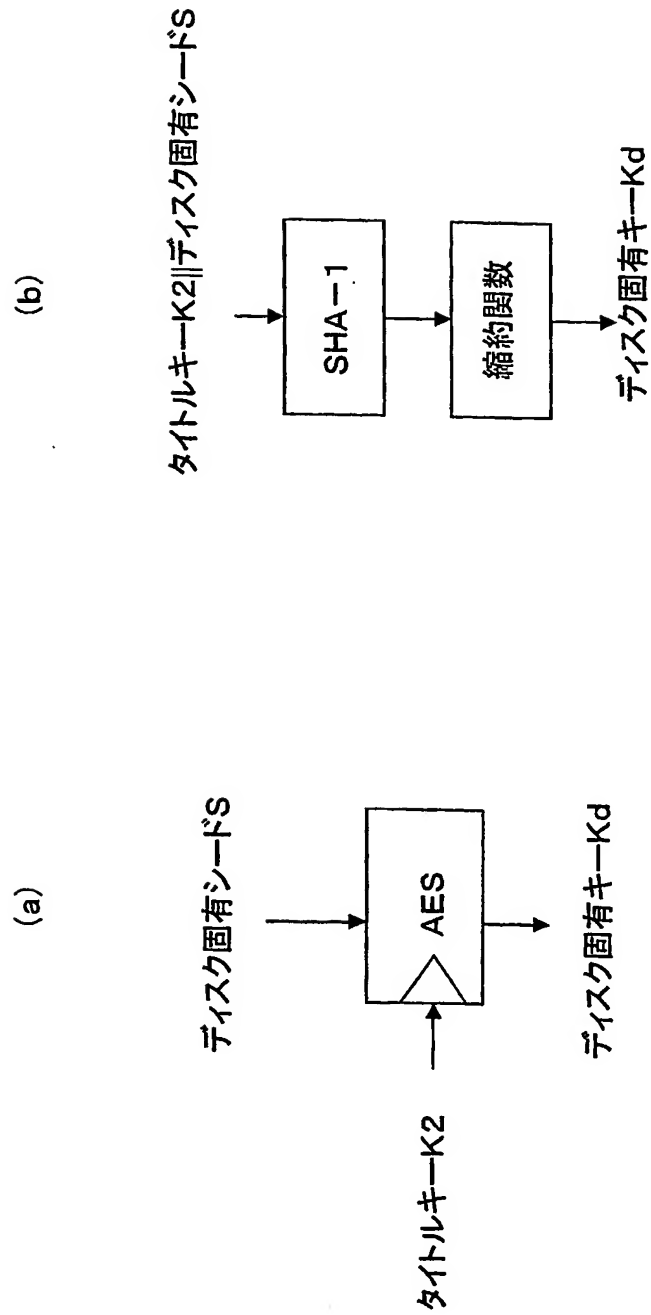
【図 9】



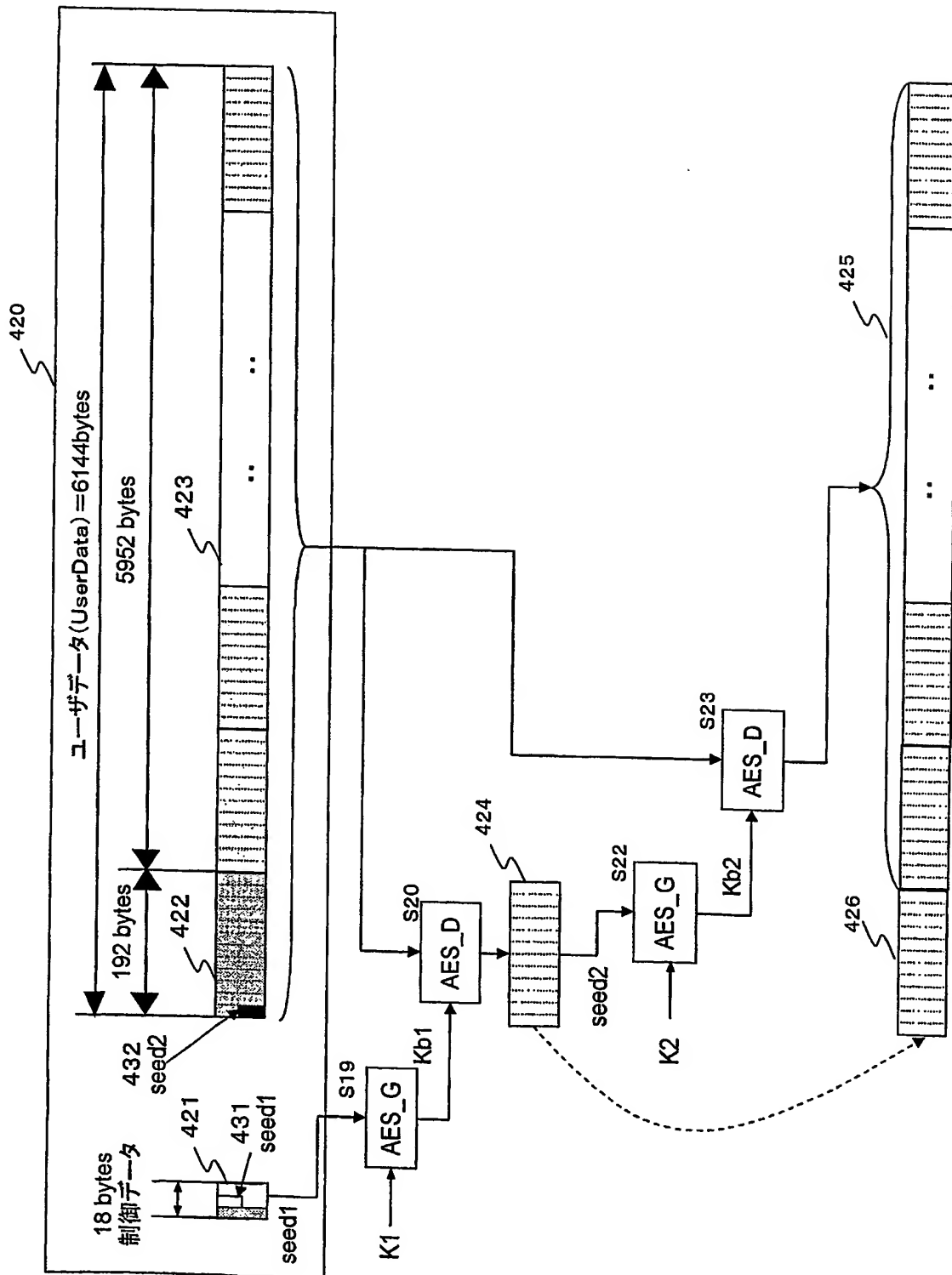
【図 10】



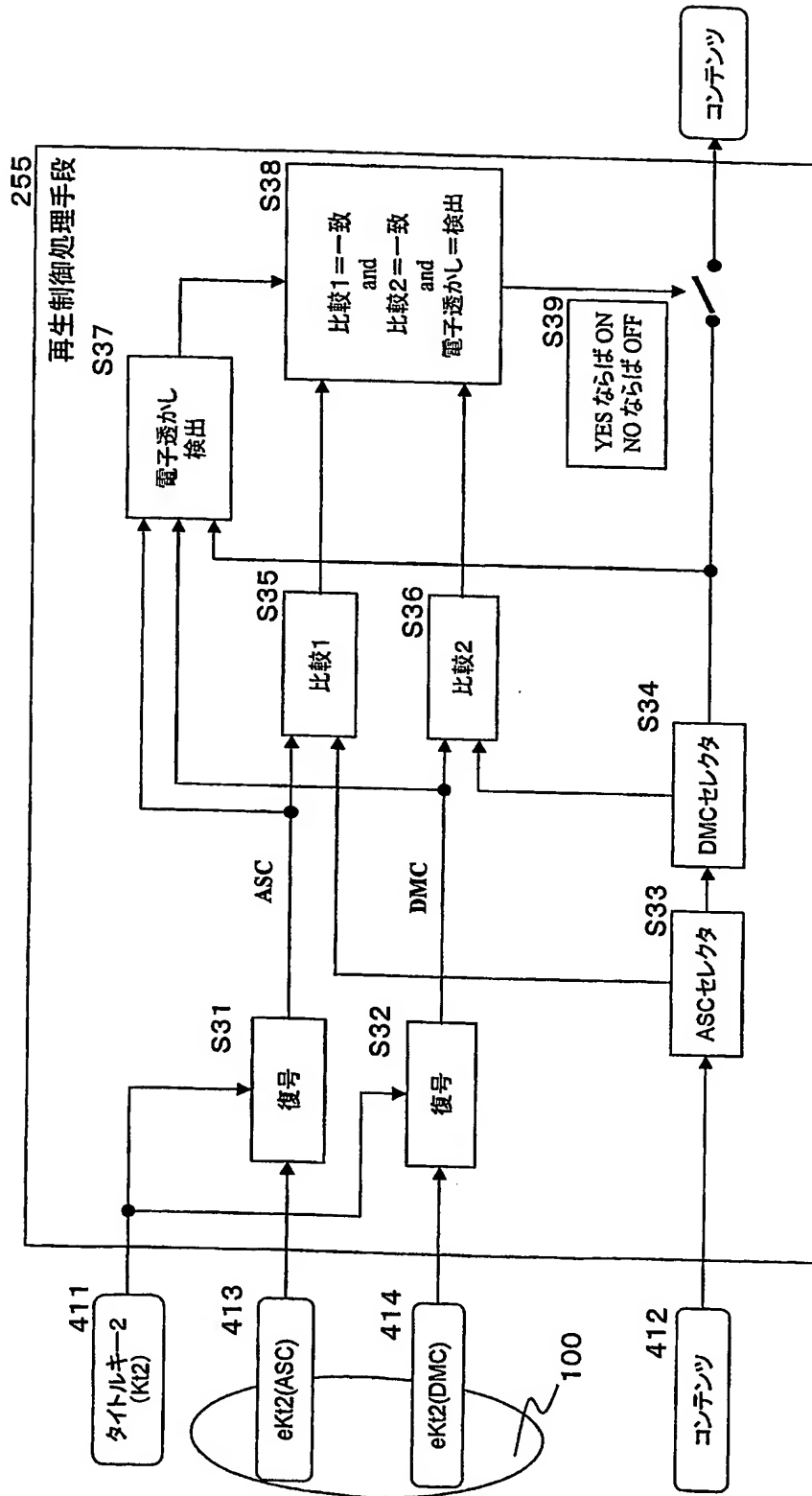
【図 11】



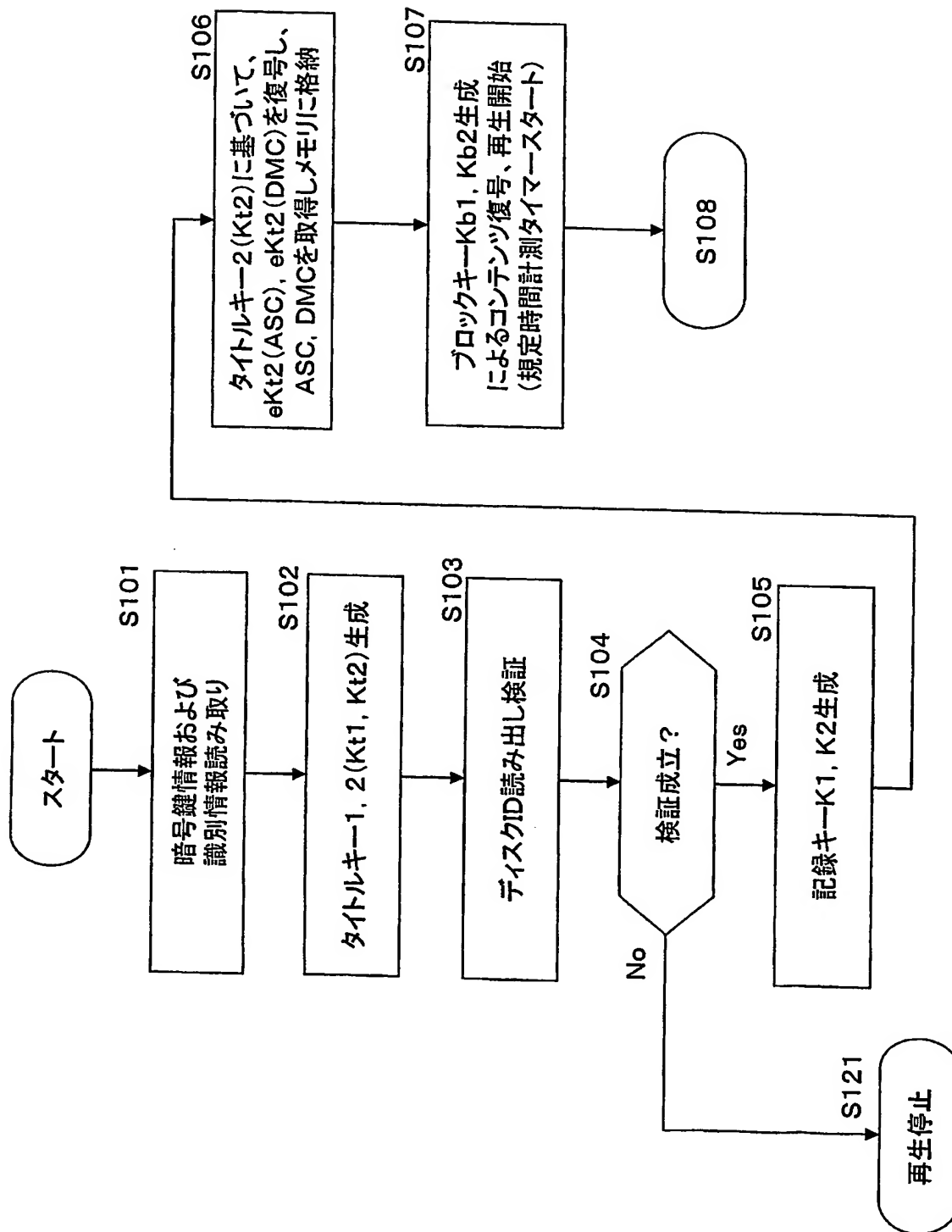
【図 12】



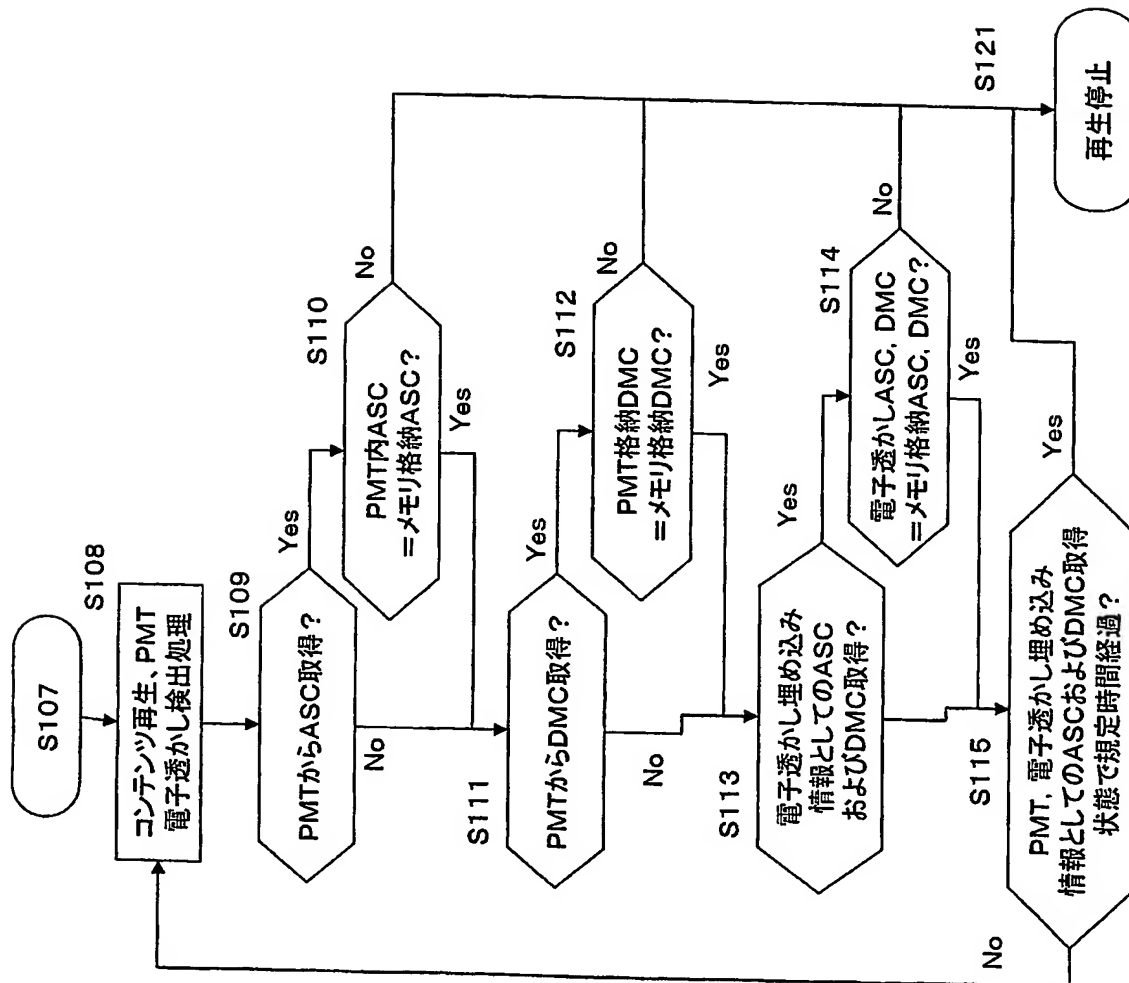
【図 13】



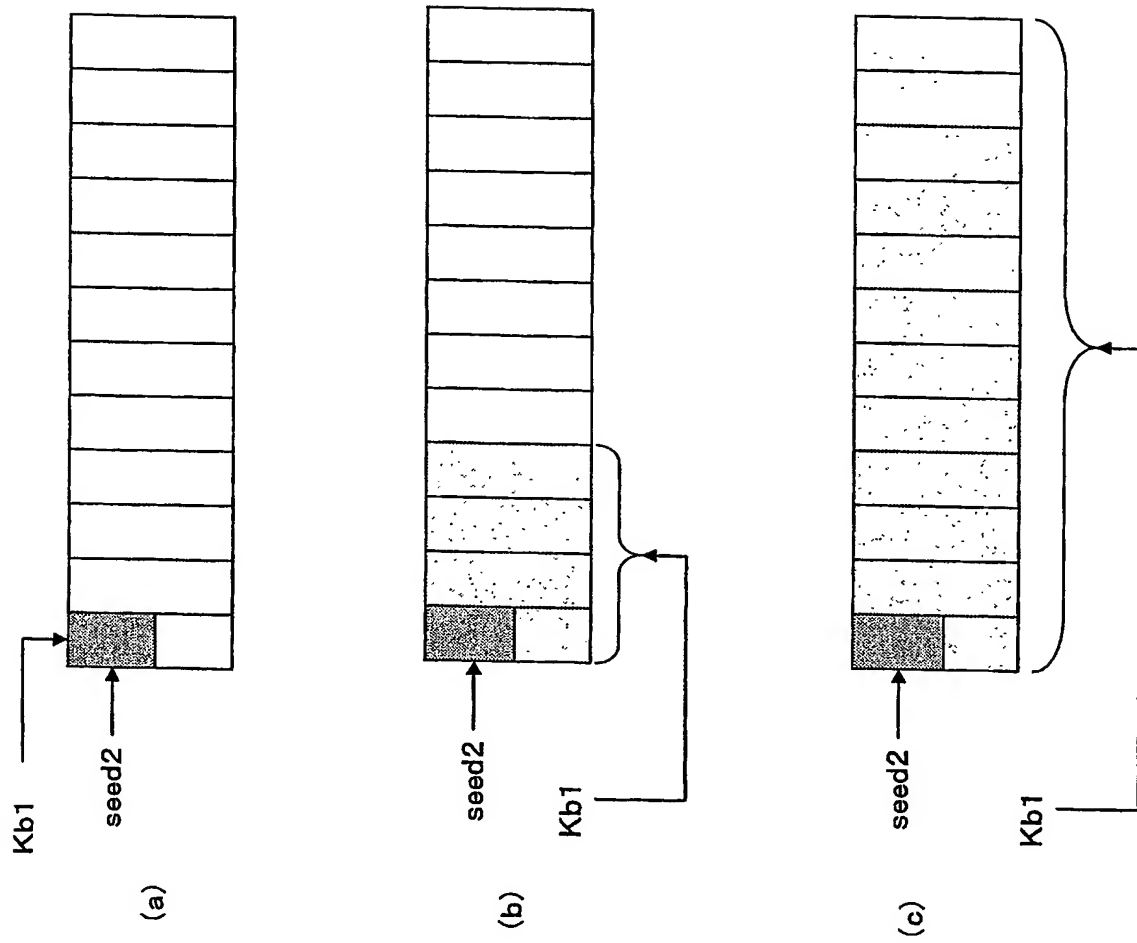
【図 14】



【図15】

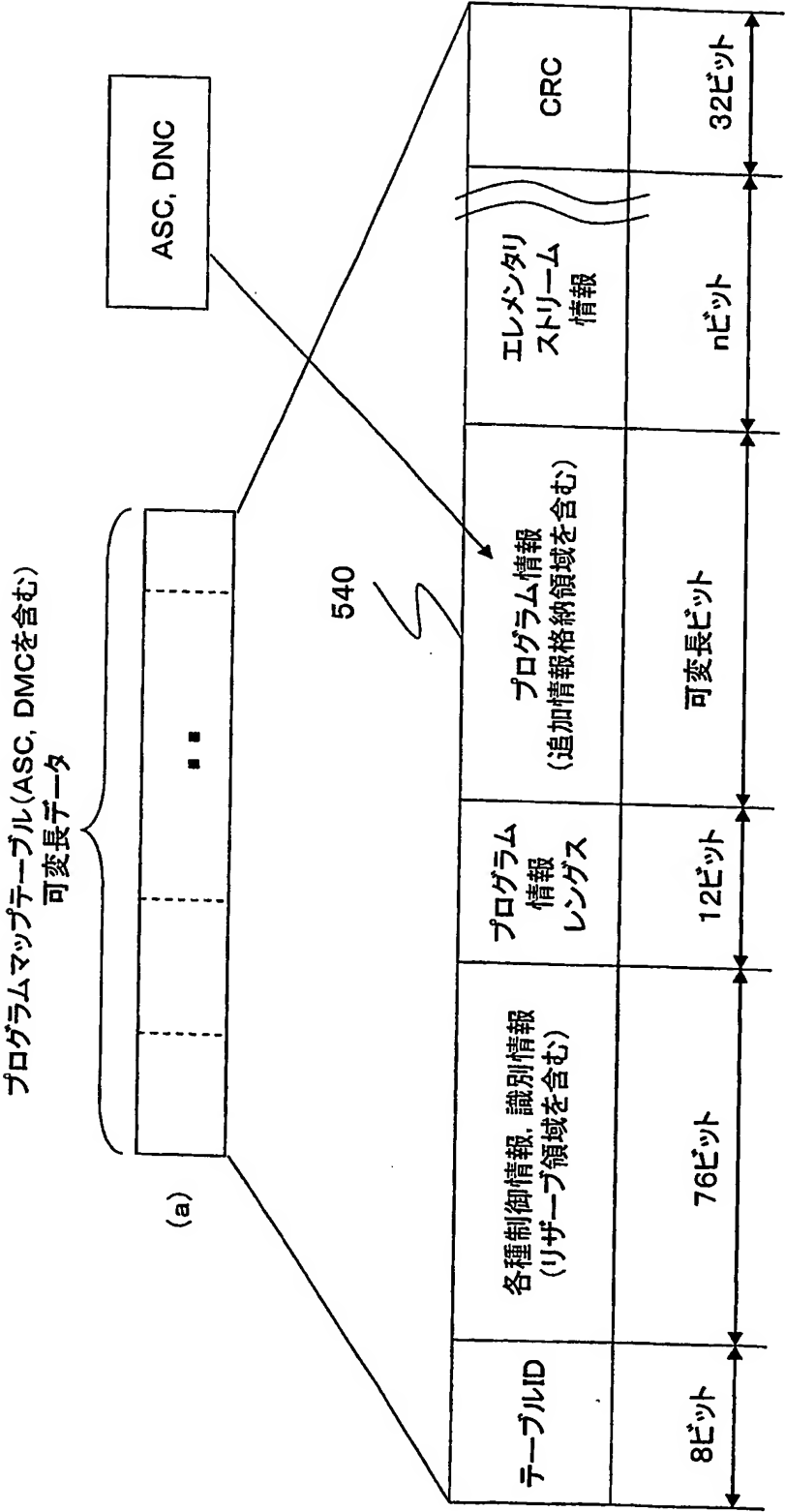


【図 16】

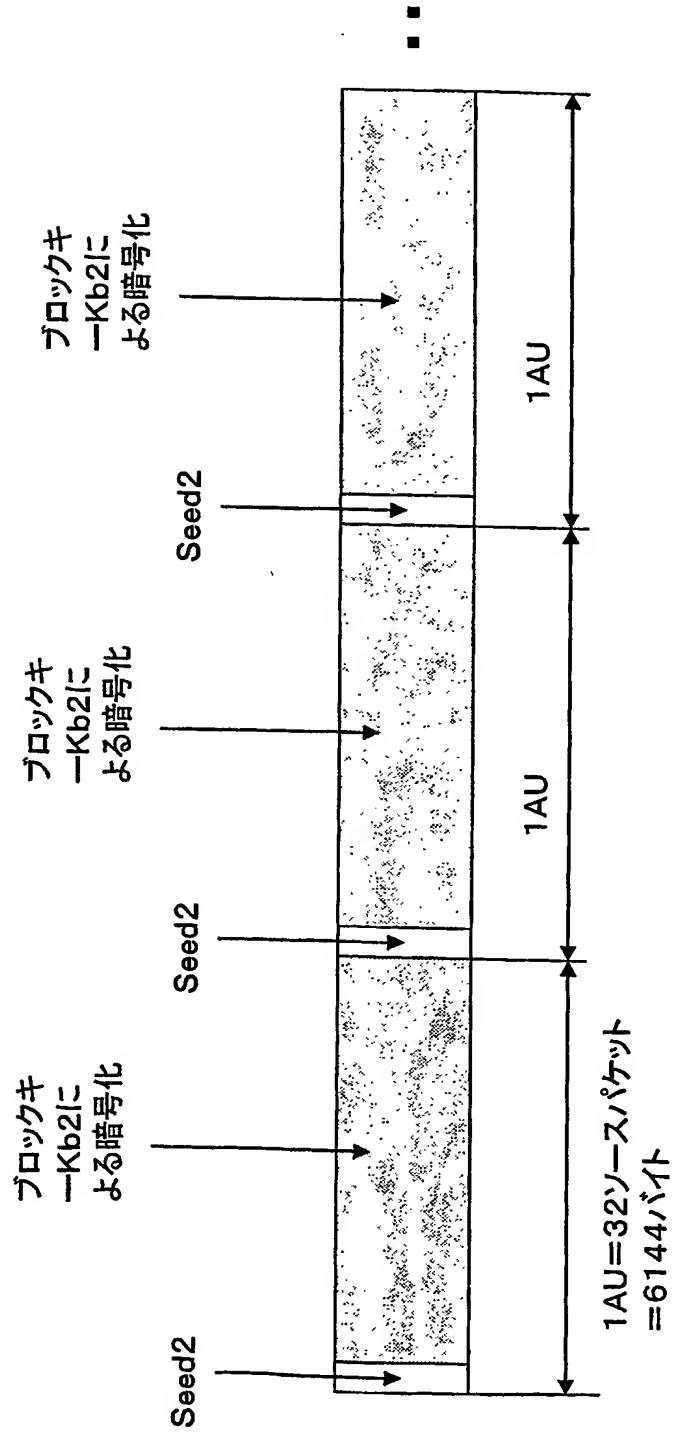




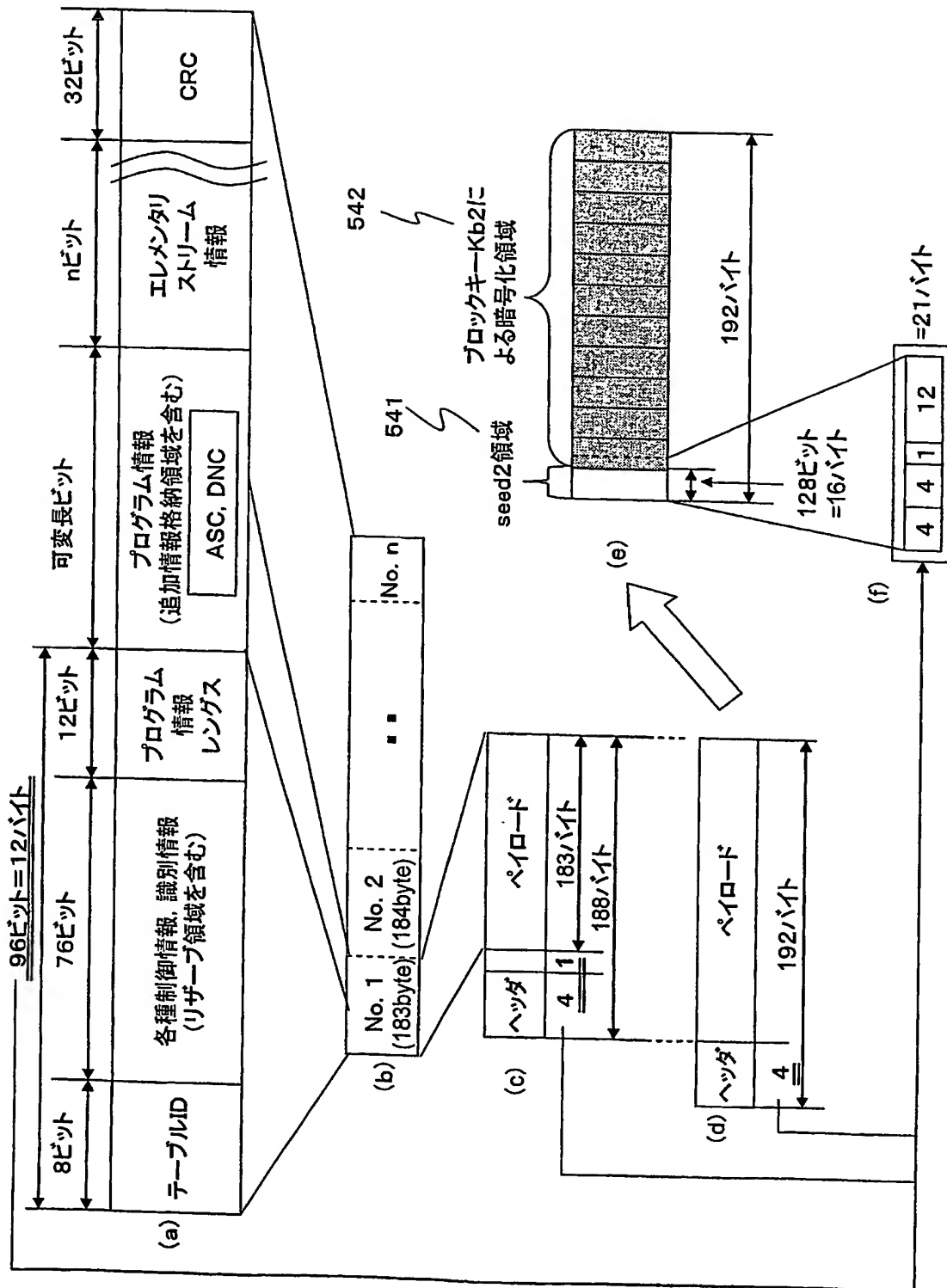
【図18】



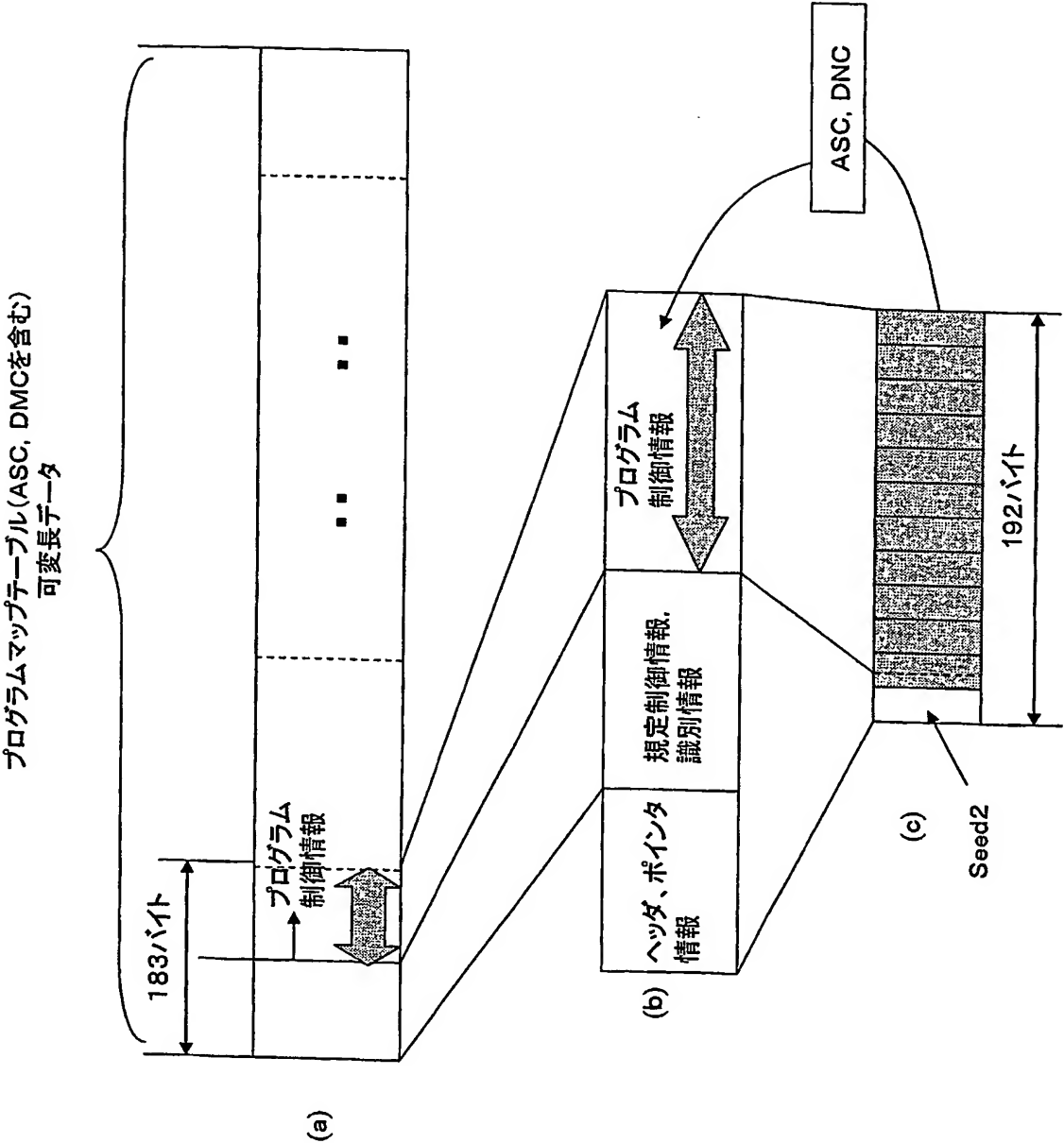
【図 19】



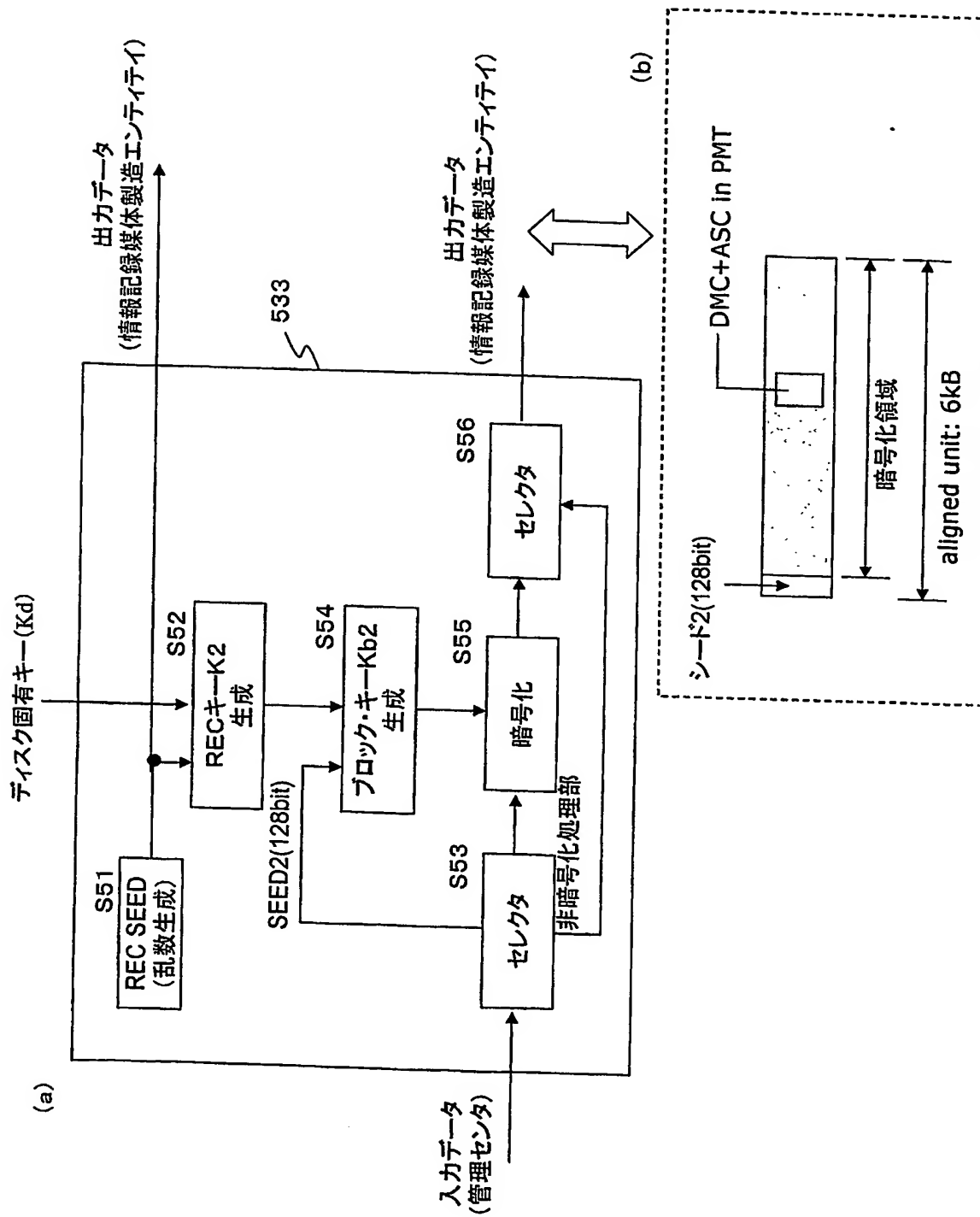
【図 20】



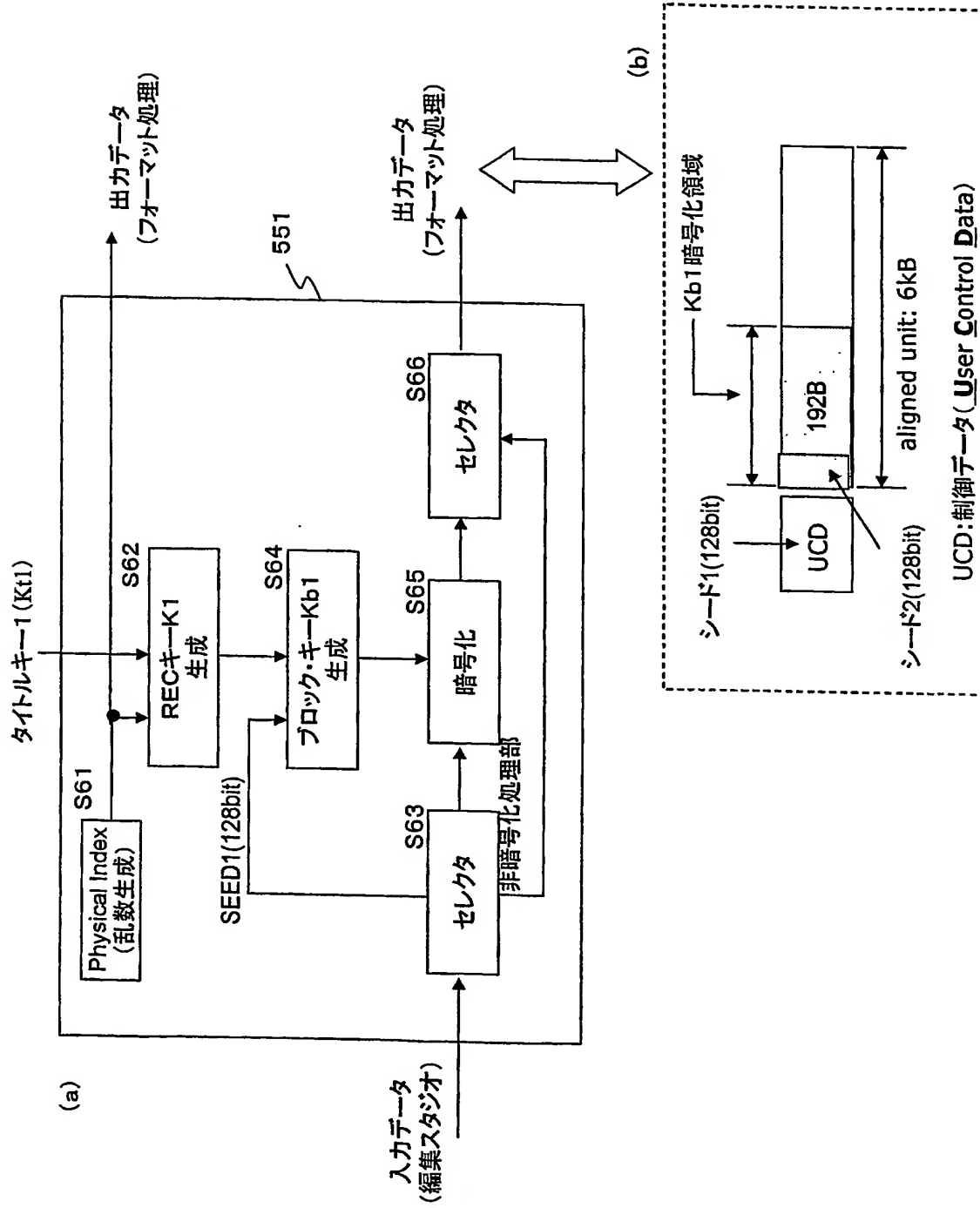
【図 21】



【図 22】

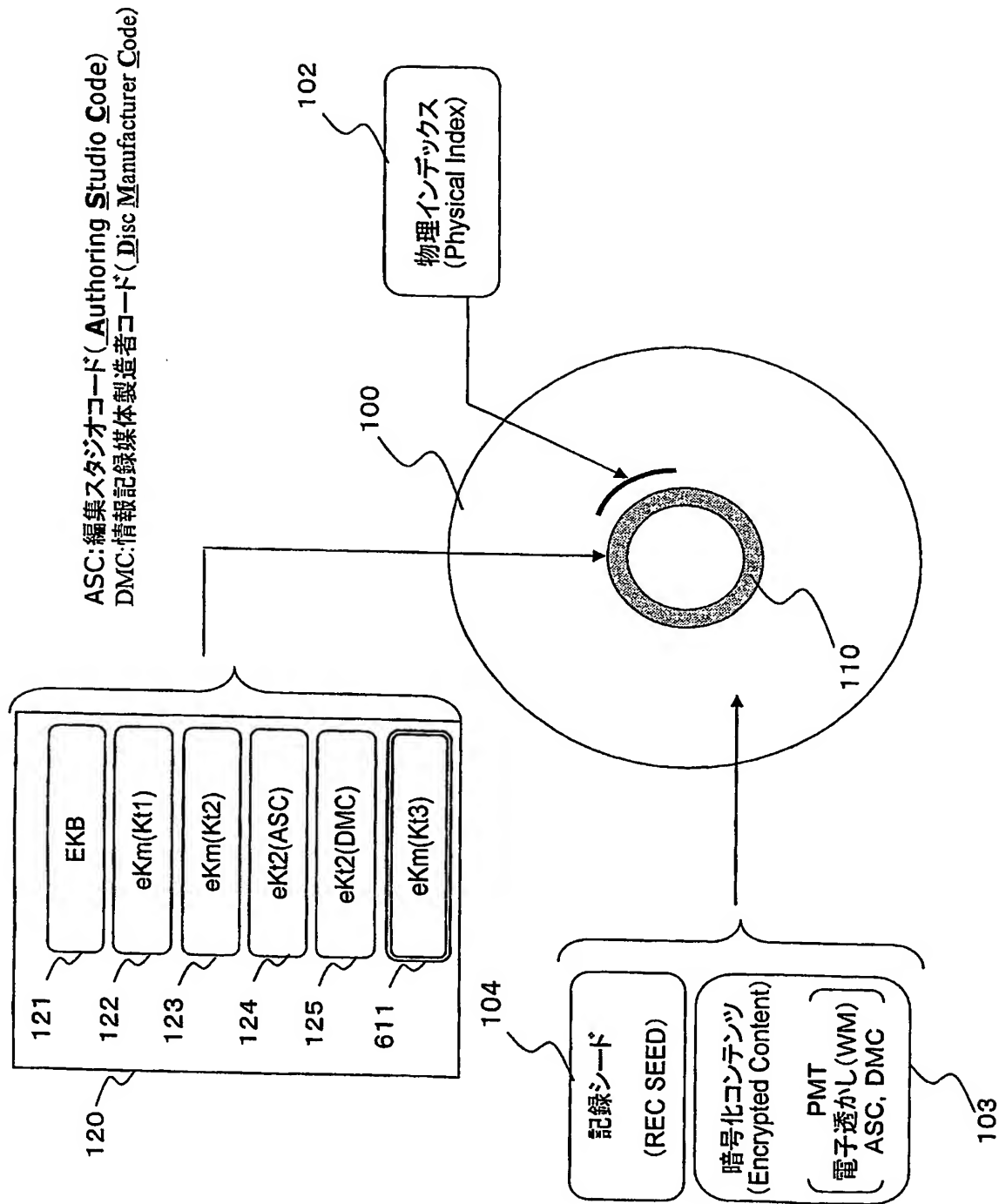


【図 23】

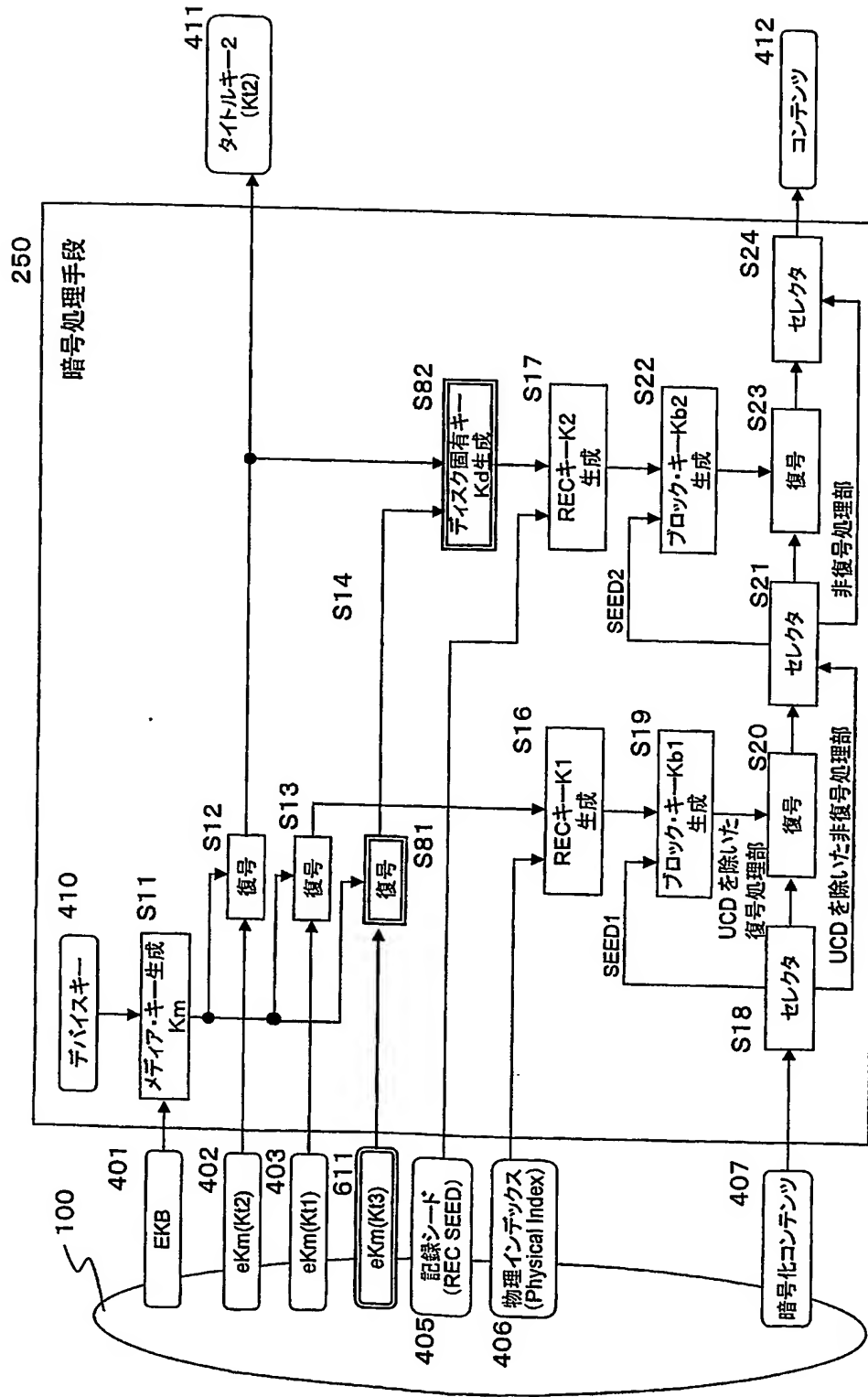




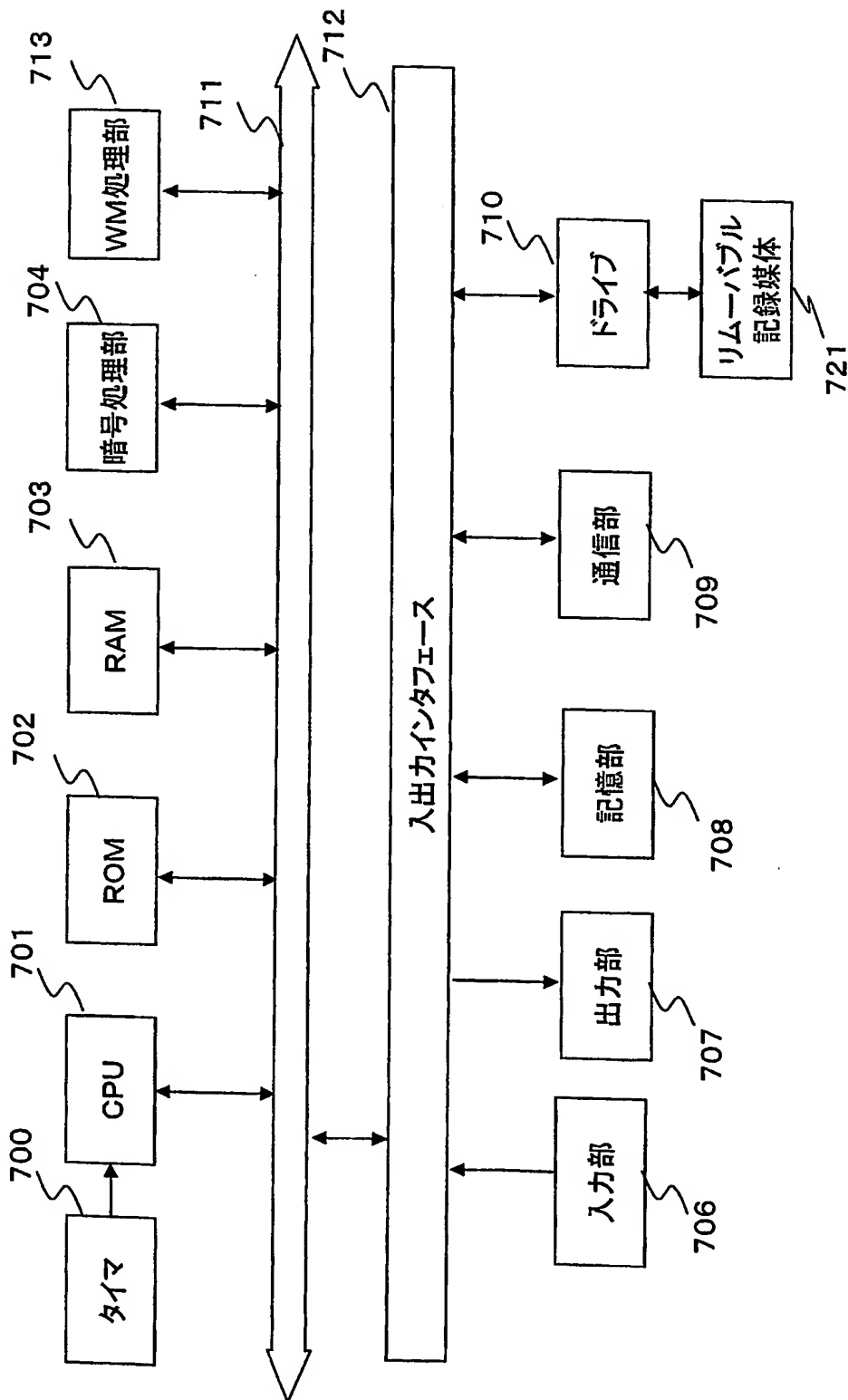
【図 25】



【図 26】



【図27】



【書類名】 要約書

【要約】

【課題】 情報記録媒体に格納される各エンティティコードの漏洩を防止した構成を提供する。

【解決手段】 編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を情報記録媒体に確実に暗号化して格納する構成とした。これらの各コードが鍵生成情報としてのシード領域に重ならないようにプログラムマッピングテーブル（PMT）内でのデータ設定位置を制御する構成としたので、編集スタジオコード（ASC）と情報記録媒体製造者コード（DMC）を格納したプログラムマッピングテーブルの格納パッケージをコンテンツパッケージ列の任意の位置に設定した場合でも、各エンティティコードが非暗号化データとしてのシード領域に重なることがなく、コードの外部漏洩を防止できる。

【選択図】 図 20

特願 2003-163723

ページ: 1/E

出願人履歴情報

識別番号

[000002185]

1. 変更年月日

1990年 8月30日

[変更理由]

新規登録

住所

東京都品川区北品川6丁目7番35号

氏名

ソニー株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**